UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

UNIDAD DE POSTGRADO

Factores inhibidores en la implementación de sistemas de gestión de la seguridad de la información basado en la NTP-ISO/IEC 17799 en la administración pública

TESIS

para optar el grado académico de Magíster en Dirección y Gestión de Tecnologías de Información

AUTOR

Alipio Mariño Obregón

Lima – Perú

2010

A mis padres, Victoria y Julián, a mis hermanos, a quienes debo todo lo que soy y seré en esta vida.

A mi esposa Socorro, a mis hijos Ali Daniel y Luis Francisco quienes son un motivo permanente para mi superación.

A mis profesores, que con sus enseñanzas y consejos me guiaron en el logro de este trabajo.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La tesis titulada “Factores inhibidores en la implementación de Sistemas de Gestión de la Seguridad de la Información basado en la NTP-ISO/IEC 17799 en la Administración Pública” es un estudio cuantitativo, transversal, hipotético-deductivo sobre el proceso de implantación de la Norma Técnica NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática del Perú.

Esta investigación, se introduce dentro del marco del desarrollo de la Sociedad de la Información, la Agenda Digital Peruana y el Proyecto de Gobierno Electrónico en el Perú y responde a la siguiente pregunta ¿Cuáles son los factores inhibidores que influyen en el bajo nivel de implementación de la Norma Técnica NTP-ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática? Para este propósito, se recopiló información a través de una encuesta semi estructurada en 16 Organismos Públicos Descentralizados adscritas a la Presidencia del Consejo de Ministros (PCM) del Gobierno Nacional, que tienen su Sede en la ciudad de Lima. La información recopilada en la encuesta, fue procesada y analizada, que permitió luego identificar factores de orden estratégico y operativo causantes del bajo nivel de implantación de la norma.

Finalmente, hemos planteado las recomendaciones orientadas a superar las dificultades que enfrentan dichas entidades, cumpliéndose de esta manera con el propósito de la investigación.

Palabras Clave: Norma Técnica Peruana (NTP-ISO/IEC 17799), Sistema de Gestión de Seguridad de la Información (SGSI), La Agenda Digital Peruana, Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Seguridad de la Información, Organismos Públicos Descentralizados (ODP).

SUMMARY

The Thesis entitled “Inhibitors factors in the Information Security Management Systems implementation based on NTP-ISO/IEC 17799 in public agencies” it is a quantitative, transversal, hypothetical-deductive method research on Peruvian Technical Norm NTP-ISO/IEC 17799 Information technology Code of practice for information security management deployment process in the National Information system Institutions of Peru.

This research, was conducted within the Information Society development framework , the Peruvian Digital Agenda and the project of E-Government in Peru, and answers the following question: What are inhibitors factors influencing the low level of implementation of the technical standard NTP-ISO/IEC 17799 code of practice for the information security management in the national system of Information institutions?. For this purpose, information was collected from a semi structured survey in 16 decentralized public bodies attached to the Presidency of the Council of Ministers (PCM) of the national Government, which have their headquarters in the city of Lima. Information collected in the survey, was processed and analyzed which allowed us then identify strategic and operational order factors causing the low-level implementation of the standard.

Finally, we raised the recommendations aimed to overcome the difficulties faced by these entities, thus fulfilling the purpose of the research.

Key Words: Peruvian Technical Norm (NTP-ISO/IEC 17799), Information Security Management Systems (ISMS), The Peruvian Digital Agenda, E-government and Informatics National Body (ONGEI), Information security, Decentralized Public Organisms (ODP).

CAPITULO 1. INTRODUCCION

1.1 Situación Problemática

El interés mundial sobre el uso y la seguridad de las Tecnologías de información y Comunicaciones (TIC), es de relevancia tanto es así que en la Cumbre Mundial sobre la Sociedad de la Información (Túnez, 2005, p.7) se declara “Pretendemos crear confianza de los usuarios y seguridad en la utilización de las TIC fortaleciendo el marco de confianza”. En el mismo documento se remarca “Subrayamos la importancia de la seguridad, la continuidad y la estabilidad de Internet, así como la necesidad de proteger Internet y otras redes TIC contra las amenazas y en sus vulnerabilidades”, así mismo en la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (NU, 2005) se expresa. “Las transacciones electrónicas no pueden desarrollarse si no hay confianza en las TIC. Las estimaciones de perjuicio económico por fallos en la seguridad alcanza decenas o quizás centenas de miles de millones cada año”.

Los retos de la administración de la seguridad de la información son enormes en los momentos actuales y serán aún mayores conforme vaya evolucionando a sistemas más complejos y sofisticados por el uso intensivo de las TICs. Por ello la seguridad es parte fundamental de las iniciativas de Gobierno Electrónico a nivel mundial. Stallings (2007) sostiene que, “Las estándares son esenciales en tales circunstancias para proveer un sistema de seguridad de la información, definición de los requisitos, alcance, políticas, métricas de gestión, monitoreo y evaluación del sistema”.

Traducido del The Internet Protocol Journal, Volume 10, No. 4, Dic 2007. Security Standars.

Nuestro país no es ajeno a la evolución de la sociedad de la información, gracias al trabajo de la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información, se cuenta con un Plan plasmada en la Agenda Digital Peruana organizada en 06 mesas de trabajo, dentro de los cuales la mesa 5 está referida al Proyecto de Gobierno Electrónico (CODESI, 2005 p.15), cuyo objetivo invoca:

> *Acercar la administración del Estado y sus procesos a la ciudadanía y a las empresas en general, proveyendo servicios de calidad, accesibles, seguros, transparentes y oportunos, a través del uso intensivo de las TICs (CODESI, 2005 p. 67)*

.

Una de las estrategias para el logro de este objetivo, consiste en desarrollar un plan de seguridad de la información en el sector público CODESI (2005), el plan antes mencionado constituye uno de los componentes fundamentales para coadyuvar a la creación de la infraestructura de Gobierno Electrónico. Consecuentemente, dada la necesidad de consolidar y estandarizar las diferentes iniciativas en el sector, el Gobierno Peruano a través de la Presidencia de Consejo de Ministros (PCM), decretó la obligatoriedad de la implantación de la Norma (NTP-ISO/IEC 17799, 2004) código de buenas prácticas para la gestión de la seguridad de la información en el sector público a partir del 23 de Julio de 2004 por Resolución Ministerial de la PCM RM N° 224-2004-PCM (2004), encargando la supervisión del cumplimiento de la implementación de la norma a la PCM a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). (NTP/ISO 17799, 2007).

La presente investigación, pretende lograr un entendimiento y determinar los factores inhibidores del proceso de implantación de la Norma Técnica Peruana (NTP) NTP-ISO/IEC 17799 código de buenas prácticas para la gestión de la seguridad de la información, dentro de las entidades

integrantes del Sistema Nacional de Informática, para lo cual se realizará un estudio cuantitativo, no experimental, transversal, hipotético/deductivo y a resultas del análisis respectivo, arribar a las conclusiones y recomendaciones que sirvan como elementos valiosos para el diseño de las estrategias más adecuadas para impulsar la implementación de la norma y por lo tanto apoyar el avance del Gobierno Electrónico en el Perú.

1.2 Declaración del Problema

El problema de investigación nace de la necesidad de llegar a un entendimiento y conocimiento en forma objetiva, sobre las diversas causas o factores inhibidores que influyen en el bajo nivel de implementación de la Norma Técnica Peruana Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática, a pesar de que desde el año 2004 la PCM declaró su obligatoriedad y extendido nuevos plazos en forma reiterada para su cumplimiento.

1.3 Objetivos

1.3.1 Objetivo General

Realizar un trabajo de investigación estudio cuantitativo, transversal, hipotético/deductivo en el Área de Gestión de las Tecnologías de Información.

1.3.2 Objetivo específico

El propósito de la presente investigación es realizar un análisis cuantitativo de las causas o factores inhibidores que han influido en el bajo nivel de implantación de la Norma Técnica NTP-ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información en las

Entidades del Sistema Nacional de Informática. La motivación que guía la presente investigación es entender las condiciones de contexto, identificar y explicar las diversas causas o factores críticos que más han influido en el retraso sufrido por las instituciones del Estado para cumplir con los objetivos del proceso de implementación de la norma. A partir de este entendimiento arribar a un conocimiento imparcial que permitirá sacar conclusiones y recomendaciones que servirán como elementos de diseño de las estrategias para mejorar la situación del proceso de implementación de la norma con el objetivo para preservar la Confidencialidad, Integridad y Disponibilidad de la información en las instituciones públicas e impulsar el desarrollo del Gobierno Electrónico como un vehículo de modernización del estado.

1.4 Justificación del Problema

Nos encontramos en un momento de profundas transformaciones sociales de enorme trascendencia y de alcance global, derivadas de la utilización masiva de las tecnologías de la información y las comunicaciones en todos los ámbitos, simbolizado a través del fenómeno de Internet. La universalización del Internet como red de comunicaciones abierta y ubicua ha creado un contexto ideal para la interacción e intercambio de la información dentro de la sociedad, en el que la seguridad de la información tiene un impacto muy grande y que atañe a todos los actores sean individuos, instituciones gubernamentales o empresas.

En la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2005) se dice “Las transacciones electrónicas no pueden desarrollarse si no hay confianza en las TIC” (pág.18).La falta de confianza de los usuarios en la seguridad de las transmisiones y transacciones electrónicas es una de las principales barreras para el desarrollo del comercio electrónico así como del Gobierno Electrónico. No se trata de una cuestión únicamente tecnológica o económica, sino fundamentalmente social y cultural que afecta a la sociedad en todos sus ámbitos de actividad. La

magnitud del problema obliga a hacer uso de la experiencia y el conocimiento acumulado en este campo, plasmados en los códigos de buenas prácticas y estándares internacionales de seguridad de la información cuyos principios fundamentales son la confidencialidad, integridad y disponibilidad; por ello en los últimos años es notable la adopción de estándares reconocidos internacionalmente y la gran aceptación que están teniendo las norma ISO 17799/ISO27002 (Ernes&young´s, 2008).

El Perú es uno de los países de la región que impulsa vigorosamente el desarrollo de la sociedad de la información, cuyos planes estratégicos están plasmados en la Agenda Digital Peruana. CODESI(2005, p.68) establece el plan de acción de la mencionada agenda, considera como uno de los objetivos estratégicos el Objetivo No 5 de Gobierno Electrónico que propone en la “Estrategia 5.1”, Acciones, numeral 6: “Desarrollo de un plan de seguridad de la información para el sector público”.

Por lo tanto, la implantación de la Norma Técnica Peruana Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática está alineado al objetivo estratégico de la Agenda Digital Peruana y es un componente importante del Proyecto de Gobierno Electrónico que permitirá a las entidades de la administración pública lo siguiente:

1. Cumplimiento con los plazos para la implantación de la norma
2. Mantener y garantizar la Confidencialidad, integridad y disponibilidad de la información en las unidades del sistema de información de la administración pública.
3. Cumplir con la legislación sobre la protección de los datos personales del administrado, registros críticos de la organización y los de Propiedad Intelectual.
4. Impulsar la implantación del gobierno electrónico para acelerar la modernización del estado.

5. Generar confianza en la ciudadanía para el desarrollo de comercio electrónico dentro de un entorno virtual seguro y cada vez más globalizado.

Lo expuesto anteriormente, muestra la relevancia que tiene la presente investigación pues nos permitirá llegar a un conocimiento objetivo de las causas, limitaciones o barreras que están dificultando la implantación y el uso de la norma dentro del sector y llegar a las conclusiones y recomendaciones que contribuya al diseño de mejores estrategias para agilizar su implementación y el cumplimiento de las resoluciones emanadas de la presidencia del consejo de Ministros en relación con la gestión de la seguridad de la información en las entidades públicas.

1.5 Naturaleza del Problema

La naturaleza de la investigación es un estudio cuantitativo, transversal, hipotético/deductivo sobre la implantación de la Norma Técnica NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática del Perú, planteándose el problema como pregunta de investigación que explique por una parte, las causas que han originado un nivel bajo en la implementación de la Norma Técnica Peruana, y por otra, los factores que dificultan su implementación, lo cual; se pretende descubrir y conocer a través de la presente estudio de investigación.

La problemática de la seguridad de la información se da en un contexto global que tiene que ver con el Gobierno de las Tecnologías de la Información en las organizaciones y que la podemos conceptualizar desde la perspectiva teórica propuesta por investigadores de la University of Antwerp Management School (De Haes S., Van Grembergen W., 2005) como un marco de procesos, estructuras y mecanismos de relación para la implementación pragmática de un marco de Gobierno de Tecnologías de Información sostenible dentro del cual se encuentra inmerso el gobierno de

la seguridad de la información orientado a la gestión de riesgos de los activos de la información y por tanto el cumplimiento de normas y regulaciones para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información dentro de la administración pública y específicamente en las Entidades del Sistema Nacional de Informática.

1.6 Pregunta de la Investigación

1. ¿Cuáles son los factores inhibidores que influyen en el bajo nivel de implementación de la Norma Técnica NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática?

1.7 Supuestos

Se asume que la ONGEI, entidad que coordina los sistemas informáticos gubernamentales continuará liderando el proyecto de Gobierno electrónico en el Perú, y que cada vez más tendrá un rol protagónico como ente articulador, promotor de la implementación de la Norma Técnica NTP-ISO/IEC 17799 con apoyo de Indecopi. entidad encargada de la Normalización en el Perú.No cambiará el apoyo político respecto al programa de modernización del estado ni la Agenda Digital Peruana.

1.8 Limitaciones

El alcance de este estudio es investigar y determinar las causas o factores que influyen en el bajo nivel de implementación de la Norma Técnica NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática.

El estudio abarcará a los Organismos Públicos Descentralizados Adscritos a la Presidencia del Consejo de Ministros del Gobierno, que es parte integrante de las Entidades del Sistema Nacional de Informática del Perú dentro del cual está inmersa la muestra elegida.

La unidad de análisis está limitada a los Directores o Gerentes que participan en la implementación de la norma.

1.9 Resumen

AlAboodi (2006), señala “Esta centuria está siendo caracterizada por términos como la aldea global, era de la información, sociedad de la información”. No hay ninguna duda que en el contexto global, la adopción masiva de las TICs, la convergencia de las infraestructuras de redes y medios ha tenido un impacto en todas los aspectos de la interacción de la sociedad, la enorme capacidad con la que hoy se cuenta para la captura, procesamiento y distribución de la información es un fenómeno sin antecedentes en la historia, estos cambios radicales en los procesos, operaciones y actividades de las organizaciones e individuos, la producción y tráfico de volúmenes enormes crecientes de información a nivel global y las amenazas proporcionales a la que están expuestas dichas operaciones, plantea un reto muy grande a los directores y administradores de tecnologías de información que tienen bajo su responsabilidad la gestión de la seguridad de la Información, por ello, los diversos actores afectados, particulares, administraciones públicas y empresas, identifican como crítico la seguridad y, en definitiva, requieren generar confianza en el uso de los sistemas de tecnologías de la información. Ministerio de Administraciones Públicas de España (2007, p.6).

Indecopi, como Organismo Peruano de Normalización aprueba las normas en todos los sectores de la actividad económica y en diversas especialidades a través de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias (CNB). Específicamente la norma

NTP ISO/IEC 17799 objeto del presente estudio fue elaborada por Comité Técnico Nacional de Codificación e Intercambio Electrónico De Datos – EDI: www. Indecopi.gob.pe (2009).

Por otra parte, la PCM a través de la ONGEI como ente rector de Gobierno Electrónico, considerando la importancia de la seguridad de la información dentro de la administración pública adopta y exige el uso obligatorio de la Norma Técnica NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática., cuya finalidad es coadyuvar a la creación de la infraestructura de Gobierno electrónico.

Sin embargo el camino en este propósito no es trivial, pues de la información obtenida hasta ahora el nivel de implantación de la norma en el sector estaría lejos de los objetivos planteados inicialmente por el gobierno y que ha sufrido retrasos en su cumplimiento y en la mayoría de los casos no se ha acometido o se encuentra en su fase de inicio (ENRIAP VI, 2007).

La aplicación del código de buenas prácticas de seguridad de la información está orientada a estandarizar los diversos proyectos y metodologías en este campo dentro del sector, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales. En la medida en que su implantación se lleve a cabo más prontamente, la aplicación de la norma y uso efectivo del mismo constituirá el fundamento para la creación de entornos seguros para la protección de la información sensible de las organizaciones e individuos dentro del estado, creando un marco de confianza para el desarrollo de los servicios en línea e interacción satisfactoria de los usuarios, impulsando de esta manera el desarrollo del proyecto de Gobierno Electrónico como parte importante de la Agenda Digital Peruana.

En el siguiente capítulo desarrollaremos el marco teórico bajo la cual se fundamente el presente estudio así como los antecedentes respecto al tema de nuestra investigación.

CAPITULO 2. MARCO TEÓRICO

La seguridad se ha convertido en uno de los problemas más urgentes para las organizaciones (Carralli, 2004). Sean estas privadas, entidades de gobierno y entidades no gubernamentales. Es un requerimiento esencial para el cumplimiento de su misión en un mundo globalmente interconectado y cada vez más informatizado (Allen, 2005). Este entorno tecnológico cada vez más dinámico y complejo que soporta los procesos y servicios del negocio, condiciona la dependencia casi absoluta de las organizaciones en la información para su desempeño efectivo en el logro de sus metas y objetivos, convirtiendo a la información en el activo clave más importante para su desarrollo, competitividad y su sobrevivencia (Lomprey, 2008).

De lo dicho anteriormente se reafirma que la información es un activo clave para las organizaciones (ISO 27001, 2005) y como tal está expuesta a amenazas que ponen en riesgo su valor, que es necesario preservar incorporando para ello los principios del Gobierno de la Seguridad de la Información como parte integral de las estrategias, procesos, personal en el marco de Gobierno de las Tecnologías de Información alineadas al Gobierno Corporativo como responsabilidad de la dirección ejecutiva .(Information Technology Governance Institute ITGI,2006).

2.1 Seguridad de la Información

2.1.1 Definición del Gobierno de la Seguridad de la información

ITGI (2006 p.17)

Es un sub conjunto del gobierno corporativo que provee dirección estratégica, asegurándose que se logran los objetivos, se gestiona apropiadamente el riesgo, uso responsable de los recursos de la organización y monitorea el éxito o fracaso del programa de seguridad empresarial.

2.1.2 Definición de la Seguridad de la Información

La definición de la seguridad de la información en el contexto de nuestro estudio lo transcribimos textualmente de la Norma Técnica Peruana NTP-ISO/IEC 17799 2007 Segunda Edición:

> *Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.*

Este concepto, se aplica en forma amplia a la información como activo de la organización al margen del medio que lo soporte que puede ser papel o los distintos tipos de dispositivos electro-magnéticos. En cualquiera de sus formas; sea texto, voz o video y durante todo el ciclo de vida de la misma (Recepción, almacenamiento, procesamiento y distribución).

2.1.3 Amenazas, vulnerabilidades y Riesgo

Amenaza, potencial de una fuente de amenaza que pueda explotar una vulnerabilidad específica ya se accidental o deliberadamente. Las fuentes más comunes de las amenazas se identifican por su naturaleza y

estas provienen de: La naturaleza, causada por inundaciones, terremotos, tormentas etc., humanas ya sean estas accidentales, por errores o deliberadas, y las ambientales como son la contaminación, fallas del suministro eléctrico prolongado etc.

Vulnerabilidad, defecto o debilidad en los procedimientos de los sistemas de seguridad, diseño, configuración o controles internos que puede ser aprovechado por alguna fuente de amenaza para atentar contra o violar las políticas de seguridad.

Riesgo, probabilidad de la materialización de una amenaza debido a la explotación de una vulnerabilidad y la magnitud de su impacto (NIST Special Publication 800-30, 2002, p12)

2.1.4 Sistema de Gestión de la Seguridad de la Información (SGSI)

En estos años han aumentado significativamente las violaciones de seguridad informática en todo el mundo (por ejemplo, la diseminación de virus y ataques que han resultado en una violación de la confidencialidad de datos almacenados), con importantes secuelas de costos en muchos casos (UIT, 2006).

En general, ante esta situación la respuesta reside en la elaboración de especificaciones suficientemente robustas para garantizar que pueden contrarrestarse las amenazas a la seguridad en cualquier esfera de la infraestructura de comunicaciones; y con el fin de poder tratar las múltiples facetas que presenta el tema de la seguridad de la información, se han creado con la participación de organismos internacionales, regionales y nacionales marcos de seguridad normalizados y códigos de buenas prácticas que proporcionen una base común que permita implementar los sistemas de gestión de la seguridad de la información en todas las organizaciones sin importar el tamaño y el sector, dando origen al concepto de la SGSI (UIT, 2006).

SGSI son las siglas utilizadas para referirse a un Sistema de Gestión de la Seguridad de la Información, una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones. El SGSI, ayuda en las empresas a establecer políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización. Para los responsables de la entidad; es una herramienta, alejada de tecnicismos, que les ofrece una visión global sobre el estado de sus sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación. Todos estos datos permiten a la dirección una toma de decisiones sobre la estrategia a seguir (INTECO, 2009).

En definitiva, con un SGSI, la organización conoce los riesgos a los que está sometida su información y los sistemas que los soporta y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente(INTECO, 2009).

Como está definido por la ISO 27001 (2005) “SGSI es parte de todo el sistema de gestión corporativa basada en riesgos del negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información”.

2.1.5 Estado del arte de la Seguridad de la Información.

2.1.5.1 Estándares y Regulaciones para la Seguridad de la Información. El fenómeno de la globalización como proceso político, económico y social en el mundo ha dado lugar al surgimiento de muchas regulaciones. Desde la directiva de la Unión Europea de protección de datos a Basel II o Sarbanes-Oxley, solo para nombrar unos pocos; las organizaciones obligadas a cumplir con estas regulaciones gubernamentales usualmente implementan marcos de trabajo reconocidos como COBIT o ISO 17799, se describe en la siguiente sección los más importantes.

2.1.5.2 Directivas Nacionales y Marcos de Trabajo sobre protección de Datos. Las siguientes directivas y Marcos de Trabajo han sido transcritos del libro The Business Case for Network Security: Advocacy, Governance, and ROI de los autores Paquet y Saxe (2004),

El derecho a la privacidad de datos personales está muy desarrollado en la comunidad Europea, e introducido en 1981 dentro del consejo Europeo. Estas iniciativas fueron seguidas por muchos países alrededor del mundo. En el Perú se trabaja la ley sobre privacidad de los datos informáticos desde Setiembre de 1999.

2.1.5.3 Ley Sarbanes –Oxley (SOX). Marco regulatorio para Gobierno corporativo, reporte financiero y control interno. La sección 404 de la ley manda, entre otros requerimientos de reporte y auditoría, que las compañías establezcan un sistema de controles internos para asegurar un adecuado reporte financiero (Agosto, 2002).

2.1.5.4 Ley de Responsabilidad y Portabilidad de los Seguros de Salud (HIPAA). El objetivo del HIPAA fue reformar el mercado de los seguros de salud y simplificar los procesos administrativos del sector salud, mientras se robustecía la privacidad y seguridad de la información de los pacientes y las entidades relacionada con la salud (Agosto, 1996).

2.1.5.5 BASEL II Accord. Establecimiento de directivas para la implementación de controles para la gestión de riesgo crediticio y operacional para el sector Bancario entró en vigor en el año 2003/2004.*Gramm Leach Billey Act (GLBA).*

También conocido como la ley de modernización del sector financiero de 1999. Incluye directivas para la creación de nuevas regulaciones sobre la privacidad y seguridad de la información de los clientes.

2.1.5.6 California Individual Privacy Senate Bill (SB 1386). Ley del Senado de California sobre la privacidad individual. Que obliga a cualquier

organización dentro del estado a notificar cualquier incidencia relacionada con la revelación de la información privada de los residentes de California.

2.1.5.7 The Federal Information Security Management Act FISMA. Ley Federal de Estados Unidos aprobada en el 2002, que manda a las agencias gubernamentales realizar una evaluación del estado de seguridad para sus sistemas clasificados y no clasificados y que incluya un análisis de riesgo y seguridad antes de la aprobación del presupuesto.

2.1.5.8 Food and Drug Administration (FDA. Regulación para la Industria farmacéutica, establece un conjunto de controles y procedimientos técnicos para el tratamiento de registros y firmas electrónicas.

Consecuentemente, han surgido también para el cumplimiento de estas normativas un grupo de estándares como:

2.1.5.9 ISO 17799. Recomendaciones de mejores prácticas sobre la Gestión operativa de la Seguridad de la información.

2.1.5.10 ISO 27001. Especificación estándar de los principales requerimientos para un sistema de Gestión de la Seguridad de la Información, contra la cual las organizaciones pueden certificar.

2.1.5.11 COBIT. Objetivos de control para la información y tecnología relacionadas. Conjunto de buenas prácticas para la gerencia de TI, usado a menudo para lograr el cumplimiento de regulaciones de las tecnologías de la información.

2.1.5.12 ITIL. Marco de trabajo muy popular para la gestión de los servicios de Tecnologías de la información.

2.1.5.13 COSO. Establece un marco de trabajo integrado y una definición común de controles internos, estándares, y criterios contra el cual las compañías y organizaciones pueden evaluar sus sistemas de control.

2.1.5.14 NIST 800. Instituto Nacional de estándares y Tecnología de los EE.UU, provee guías para la seguridad de los recursos de información basados en computadora, explicando conceptos importantes, consideración de costos e interrelación de los controles de seguridad.

2.1.5.15 ISO 13335. ISO 13335 es un compendio de 5 documentos que de forma práctica aborda la seguridad de las Tecnologías de la Información y orienta sobre los aspectos de su gestión, describiendo aspectos conceptuales, gestión, planificación, selección de controles y la seguridad de las redes.
ISO 15408.

2.1.5.16 **La norma ISO 15408.** Define los criterios comunes de seguridad que las tecnologías de la información deben respetar. Estos criterios comunes permiten la evaluación de las funciones de seguridad a través de once clases funcionales y exigencias de garantía entre ellos la auditoria, la comunicación, soporte criptográfico etc.

2.1.6 Evolución y tendencias de la seguridad de la Información

En los resultados de 2006, la Encuesta Global sobre Seguridad de la Información de Ernest & Young pone de manifiesto que durante los pasados años muchas empresas han realizado progresos notables en la reducción de riesgos, reforzando la seguridad de la información habiendo realizado mayores inversiones en tecnología, procesos y personal con el fin de garantizar los principios de la seguridad de la Información (Ernest & Young's, 2006).

Para la correcta administración de la Seguridad de la Información, se deben establecer y mantener programas que busquen preservar los tres principios de la seguridad de la información: La confidencialidad, la integridad y la disponibilidad (NTP-ISO/IEC 17799, 2007); definidos así: a) Confidencialidad: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional de la información. La pérdida de la

confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización, b) Integridad: Busca asegurar, que no se realicen modificaciones por personas no autorizadas a los datos, información o procesos, que los datos o información sea consistente tanto interna como externamente. c) Disponibilidad: Busca el acceso confiable y oportuno a los datos, información o recursos para el personal apropiado (NTP-ISO/IEC 17799, 2007).

2.1.7 Código de buenas prácticas de Seguridad de la información: ISO 17799

Código de buenas prácticas o mejores prácticas como está definida por la Oficina de Contabilidad General de los Estados Unidos (USGAO), "Son los procesos, prácticas y sistemas identificados en las organizaciones privadas y públicas que funcionaron excepcionalmente bien y son ampliamente reconocidos como una mejora de performance y eficiencia en áreas específicas" (Stevenson y Romne, 2004).

Los rápidos cambios producidos en la sociedad por el uso de la informática, enfrenta a las organizaciones; a grandes retos en relación a la seguridad de la información a fin de mitigar los riesgos inherentes relacionados, lo cual ha estimulado en los últimos años la adopción creciente de estándares reconocidos y de gran aceptación internacionalmente, entre ellos la ISO 17799, ISO 27002/27001 (Ernest&Young's, 2008).

La historia del ISO 17799 se remonta a un código de práctica publicado por el Gobierno del Reino Unido el Departamento de Comercio e Industria (DTI) en 1989, el mismo está basado primordialmente en una estándar de seguridad interna usado por una compañía de Petróleo (Paquet, Saxe, 2004). En el siguiente cuadro de la figura 1 se presenta la cronología de la evolución del estándar que es la más ampliamente conocida y aceptada internacionalmente.

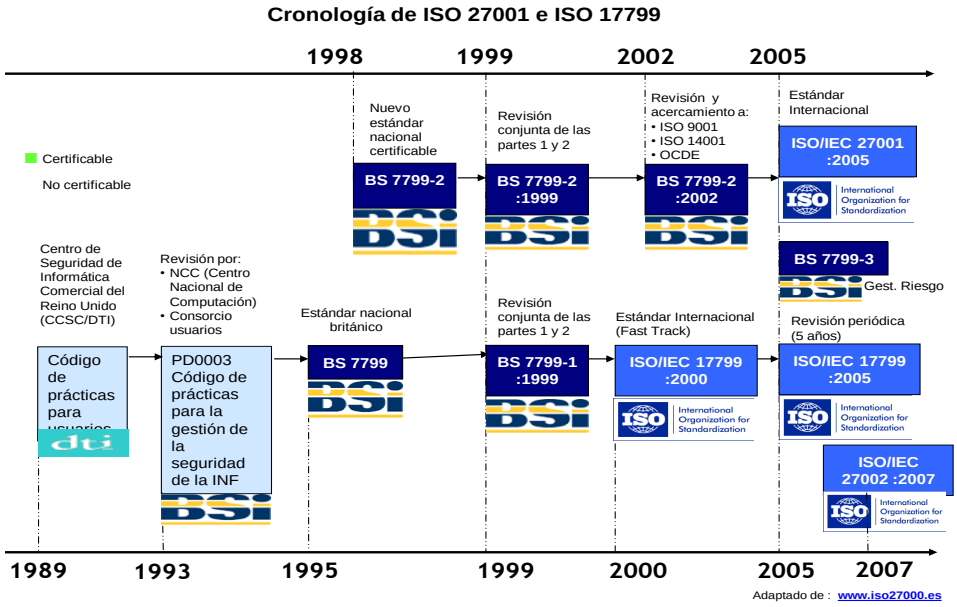

Grafico 1. **Evolución del estándar de Seguridad de la información**
Fuente: www.iso27000.es

La madurez de las actividades de Gestión de Seguridad de la Información en las organizaciones dio un gran paso con la publicación en 2005 del estándar ISO 27001, primer y principal estándar certificable de la familia 27000, orientada a este campo.

La familia 27000 a partir del año 2000 consolida y estandariza a nivel internacional las diversas iniciativas nacionales que estaban en aplicación desde el final de la década de los noventa, como la serie BS: 7799-1, BS: 7799-2 en Reino Unido. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. Aunque la más popular de todas ellas era la norma ya internacional, ISO 17799. Esta norma se ha reenumerado en 2007 en la Norma ISO 27002, dentro de la familia 27000. Todas estas iniciativas se vienen aplicando con éxito en los últimos años en múltiples países (70) y organizaciones (The ISO Survey, 2007). Así, a finales de 2006, existían cerca de 3000 organizaciones en el mundo que habían obtenido su certificación de seguridad, mediante la implantación y certificación de su Sistema de Gestión de Seguridad de la Información.

2.1.8 Metodologías de Implementación

2.1.8.1 El modelo cíclico Plan Do Check Act (PDCA). Según Eloff y Eloff (2003), Los SGSI se definen en sus dos aspectos: proceso y producto. Como producto es un sistema de administración que la organización adopta para establecer y mantener la seguridad de la información, como proceso es un sistema iterativo con realimentación y mejora contínua que sigue el modelo Plan Do Check Act (PDCA). Este es uno los modelos más populares, base para todos los Sistemas de Gestión incluyendo el de la Seguridad de la Información, y se apoya en la necesidad de que la Seguridad de la Información esté en continua evolución; además, dicha evolución esté documentada y justificada. Tiene cuatro fases. (Figura No 2):

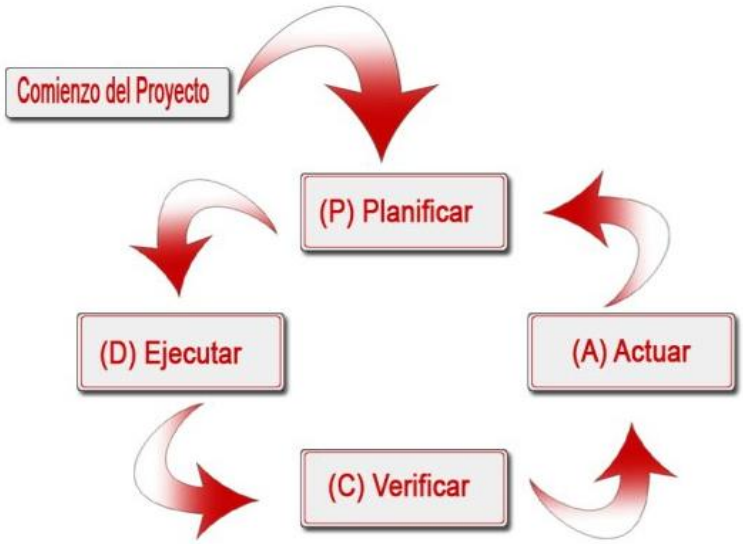

Grafico 2. **Diagrama de la metodología PDCA, Fuente: Instituto Nacional de Tecnologías de la Comunicación (INTECO).**

2.1.8.2 Planificar. En esta primera fase se realiza un estudio de la situación de la Organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar en función de las necesidades detectadas.

Hay que tener en cuenta que no toda la información de la que dispone la organización tiene el mismo valor, e igualmente, no toda la información está sometida a los mismos riesgos. Por ello un hito importante dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo se hace necesario una Gestión para dichos riesgos de cara a reducirlos en la medida de lo posible.

El resultado de este Análisis y Gestión de Riesgos será establecer una serie de prioridades en las tareas a realizar para minimizar dichos riesgos. Puesto que los riesgos nunca van a desaparecer totalmente, es importante que la Dirección de la Organización asuma un riesgo residual, así como las medidas que se van a implantar para reducir al mínimo posible dicho riesgo residual.

2.1.8.3 Ejecutar. En esta fase se lleva a cabo la implantación de los controles de seguridad escogidos en la fase anterior. En dicha implantación se instalarán dispositivos físicos (HW, SW), pero también se creará o revisará la documentación necesaria (políticas, procedimientos, instrucciones y registros).

Dentro de esta fase es muy importante dedicar un tiempo a la concienciación y formación del personal de la empresa de cara a que conozcan los controles implantados.

2.1.8.4 Verificar. Es importante que la Organización disponga de mecanismos que le permitan evaluar la eficacia y éxito de los controles implantados. Es por esto que toman especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

2.1.8.5 Actuar. En esta fase se llevarán a cabo las labores de mantenimiento del sistema así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se suele

llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se suele esperar a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

2.1.9 Modelo Six Sigma

Este modelo se basa en las siguientes fases: Define, Mida, Analice, Mejore y Controle de sus siglas en inglés (DMAIC), se enmarca dentro de la perspectiva de los dominios de la Estrategia, Tecnología, Organización, Personas y Ambiente de sus siglas en inglés (STOPE). En ambos casos se persigue la gestión de la Seguridad de la Información como un proceso de mejora contínua (Saleh, Alrabiah y Bakry, 2007).

2.1.10 El Factor Humano

La Tendencia creciente de la adopción de la norma Internacional de Seguridad de la información y la certificación de los Sistemas de Gestión bajo los requisitos de la ISO/IEC 27001, dio lugar a un mercado orientado a la formación de especialistas en auditoría interna y auditores líderes en la Norma impartidas por Instituciones acreditadas como AENOR, SGS, Bureau Veritas entre los más destacados; convirtiéndose en una práctica creciente que se complementa con el otorgamiento de Certificaciones a profesionales en Seguridad de la Información.

Los sistemas de certificación disponibles, son administrados por organismos de la industria generalmente sin fines de lucro entre los principales está; el Instituto de Profesionales de la Seguridad de la Información sus siglas en Inglés (IISP), La asociación de Auditoria de Sistemas de Información y Control sus siglas en Ingles (ISACA). El programa más general es la certificación CISSP**.** Otros, como CISM y CISA orientadas a la certificación de los administradores de seguridad y los auditores, son los más reconocidos internacionalmente.

2.1.11 Marco Legal y hechos importantes

2.1.11.1 Masificación del Internet: e-Perú. El 6 de Junio del 2001, mediante el decreto supremo DS N° 066-2001-PCM Se creó la Comisión Multisectorial para Masificar el uso de Internet en el Perú. Esta comisión en un esfuerzo conjunto con la participación del Sector privado efectuó un diagnostico preliminar y delineó las políticas generales para masificar el uso del Internet cuyo resultado se plasmó en el documento denominado "e-PEru" Propuestas para un Plan de Acción para el Acceso Democrático a la Sociedad Global de la Información y el Conocimiento y luego en el 2003 la creación de la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información en el Perú que dio lugar a la Agenda Digital Peruana (CODESI, 2005).

2.1.11.2 Mesa CODESI 5. Gobierno Electrónico Encargada de formular estrategias y recomendaciones para mejorar la eficiencia, transparencia y eficacia de la administración pública al servicio de las personas con el desarrollo, la implementación y la sostenibilidad del gobierno electrónico, y las nuevas aplicaciones generadas por las TICs en la Sociedad de la Información.

2.1.11.3 Creación de la ONGEI. En junio del 2003, mediante Decreto Supremo Nº 066-2003-PCM se crea en la Presidencia del Consejo de Ministros, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), con el encargo de liderar y articular el proyecto de Gobierno Electrónico dentro del Sistema Nacional de Informática. La ONGEI tiene entre sus funciones:

a) Proponer la Política Nacional de Gobierno Electrónico e Informática del Estado en concordancia con el Plan para el Desarrollo de la Sociedad de la Información en el Perú elaborado por la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI); b) Proponer la normatividad y coordinar el desarrollo del Gobierno Electrónico y de la

actividad informática en la Administración Pública, impulsando su modernización; c) Elaborar y desarrollar la Estrategia Nacional de Gobierno Electrónico y coordinar y supervisar su ejecución; d) Coordinar y supervisar el desarrollo de los portales de las entidades del sector público, con el fin de establecer la ventanilla única de atención a las empresas y ciudadanos.

2.1.11.4 Resolución Ministerial No. 224-2004-PCM. Presidencia de Consejo de Ministros- Gobierno del Perú- ONGEI. Aprobación de la Norma Técnica Peruana NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática.

2.1.11.5 Resolución Ministerial No. 395-2005-PCM. Presidencia de Consejo de Ministros- Gobierno del Perú- ONGEI. Modificación plazos para implementar la Norma Técnica Peruana cuyo uso obligatorio se aprobó mediante las R.M. No. 224-2004-PCM.

2.1.11.6 P01-PCM-ISO17799-001-V1. Presidencia de Consejo de Ministros- Gobierno del Perú- ONGEI Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información 1ra. Edición NTP-ISO/IEC 17799: 2004.

2.1.11.7 R.001-2007/INDECOPI-CRT. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información 2da. Edición NTP-ISO/IEC 17799: 2007. Es la versión vigente de la Norma Peruana en reemplazo de la norma anterior que esencialmente es el mismo. La Norma fue elaborada por el Comité técnico Permanente de Codificación e Intercambio Electrónico de Datos (EDI),durante los meses de Junio y Julio del 2,006. Utilizó como antecedentes la Norma ISO/IEC 17799: 2005. Information Technology – Code of practice for information security management.

2.1.11.8 Implementación del Portal de la ONGEI en el año 2003*:* Esta implementación incorpora una página Web dedicada a difundir la NTP

ISO/IEC 17799, así como documentos y herramientas sobre la seguridad de la información entre las entidades del estado. Así mismo, desarrolla y publica en su portal un modelo simplificado para la aplicación de la Norma en la administración pública que consta de cuatro etapas a saber:

2.1.12 Etapas del Modelo Simplificado de Implementación

Descripción de las etapas:

2.1.12.1 Etapa I. Esta primera etapa consiste en analizar la misión, visión y objetivos de la organización.

***2.1.12.2 Misión y Visión y Objetivos de la Organización*.** La misión y visión dan el enfoque claro de lo que la organización debería plantearse en términos de seguridad de la información de manera general.

2.1.12.3 Identificación de los recursos dentro de los procesos de la organización. El análisis de las principales funciones dentro de los procesos de la organización nos permitirá identificar todos los recursos que interactúan en estos procesos, los cuales podemos clasificarlos de la siguiente manera:

2.1.12.4 Los recursos materiales y tecnológicos involucrados. Recursos Humanos. Como resultado de esta etapa se tiene que tener una matriz con las funciones y todos los recursos o activos de información involucrados dentro del proceso analizado.

2.1.13 Etapa II

En esta etapa debemos de usar la información obtenida de la Etapa I, para implementar lo que se recomienda dentro de la NTP-ISO/IEC 17799.

2.1.13.1 Establecimiento de la Política de Seguridad de La organización. Se establecerá la política general a nivel de toda la

organización, a partir de esta política se desarrollarán las normativas internas y procedimientos específicos, para cada área dentro de la empresa con el fin de cumplir con la política general.

***2.1.13.2 Efectuar un análisis de riesgos*.** En base a los activos identificados en la Etapa I, se comenzará a elaborar un análisis de riesgos, con la finalidad de poder identificar las vulnerabilidades, amenazas e impacto de estos sobre los activos identificados. En base a los controles establecidos para cada dominio de la Norma que permita establecer la Brecha.

El análisis de riesgos nos permitirá priorizar cuales son los activos prioritarios a proteger, y en base a esto realizar una comparación de lo que ya se tiene implementado versus lo que falta implementar, como medidas de seguridad.

2.1.14 Etapa III

En esta etapa se tiene que proyectar la implementación de lo que se necesita en términos de seguridad.

Documentación del Plan de Seguridad de la Información

Establecimiento del documento del plan a 1, 2 o 3 años.

2.1.15 Etapa IV

Una vez elaborados los pasos anteriores se definen como entregables los siguientes documentos:

Política de Seguridad

Análisis de riesgos

Brecha de lo implementado y lo que falta por implementar

Plan de Seguridad de la Información : (PCM/ONGEI- Portal: Políticas de Seguridad-Modelo Simplificado).

2.2 Antecedentes del Problema

2.2.1 Adopción e implementación de la ISO/IEC 17799 en el mundo y estudios Previos.

En el mundo, son 70 los países que han adoptado la norma ISO 27001, cuyo pre-requisito para su certificación es el ISO 17799 (The ISO survey, 2007). Según la página WEB de Certificaciones ISO 2700 (Tabla No 18), Japón encabeza los países con el mayor número de certificaciones del SGSI (3,572), seguida por India (490) y Reino Unido (448) . En Latinoamérica: México (24), Brasil (23), Colombia (8) y Chile (3), Perú (3) y Argentina aparecen con (02) certificaciones.

De Junio hasta octubre de 2007, PricewaterhouseCoopers (PwC, 2007) por encargo el Instituto de Gobierno de TI (ITGI) realizó una encuesta a nivel mundial cuyo resultado se publica en el estado Global de Gobierno de TI, Reporte 2008 enfocado a riesgos de TI y entrega de valor. En este reporte se puede apreciar específicamente el uso de estándares y mejores prácticas; observándose que el uso de ISO 17799/ISO 27000/ISO TR13335/ISF o estándar equivalente de seguridad, en el gráfico que reproducimos; entre el 2005 y el 2007 creció de 9% en el 2005 a 10% en el 2007.

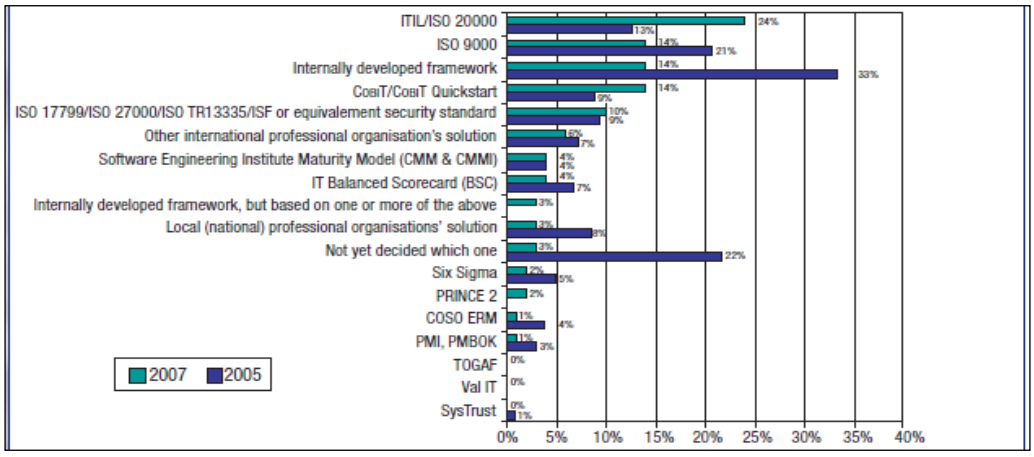

*Grafico 3. **Marcos de trabajo seleccionados en uso a nivel mundial***

Fuente: **PricewaterhouseCoopers (PCW, 2007)**

Otro estudio Internacionalmente importante revisado es, una investigación titulada “Critical success factors and requirements for achieving business benefits from information security” (Partida, Ezingerad, 2007). Realizado en Henley Management College de Reino Unido por Alberto Partida y Jean-Noël Ezingeard.

En el mencionado estudio, a través de una encuesta a más de 80 profesionales de la seguridad de la información y expertos a nivel mundial se muestra que las organizaciones que desarrollan prácticas de seguridad de la información en base a un fuerte compromiso de la alta dirección, integrando sus procesos de administración de riesgos incluyendo la seguridad de la información alineados a los objetivos estratégicos, obtienen beneficios superiores. En este mismo estudio, se señala que los tres beneficios más comunes son: Valor incremental para los accionistas, nuevas oportunidades de negocios y mejor gobierno (cumplimiento).

En cuanto a los factores que determinan el éxito de los programas de seguridad de la información el estudio agrupa bajo dos temas principales: (1) Los procesos de administración y las responsabilidades y (2) Alineamiento.

Bajo estos dos temas se identifican ocho (08) factores críticos, los cuales fueron contrastados también con el enfoque de varios autores o Instituciones quienes identifican algunos de ellos en sus investigaciones, cuyo resultado se reproduce en la tabla No 1:

*Tabla 1.***Factores críticos de éxito de la seguridad de la información**

Ítem	Tema 1: Proceso de administración y responsabilidades	
1	Obtener el compromiso de la alta dirección	ISO (2004 y "2005); COSO (2004); Appel (2005) y Ezingead et al (2004)
2	Establecer un programa para mejorar la gestión de la Seguridad a través de toda la organización y reforzarlo	Straub (1998), ISF (2005a)
3	Adopte una estándar	May (2003), Von Solms (2005a)
4	Comunique el valor para el negocio de la seguridad de la información en un lenguaje común de riesgo	Scholtz (2004b y 2004c), Coles y Moulton(2003)
5	Determine el propietario del riesgo en forma indubitable	Coles y Moulton(2003)
	Tema 2 : Alineamiento	
6	Refleje los objetivos del negocio en los elementos de seguridad de la información	Birchall et al. (2004), Scholtz (2004a), ISO (2005).
7	Alinee la seguridad de la información con los sistemas Informáticos y las estrategias generales	Booker (2006), Leskela et al. (2005), Birchall et al. (2003)
8	Sea consistente dentro de la cultura organizacional	Birchall et al. (2004), Scholtz (2004a), ISO (2005).

En nuestro estudio, tomamos como referencia para el diseño del modelo de investigación por analogía al referido estudio a fin de plantear la hipótesis correspondiente la cual se expone en el capítulo correspondiente.

En el caso norteamericano, la ley Federal de Gestión de seguridad de la información (FISMA) fue aprobado por el congreso norteamericano en el año 2002 (OMB, 2008) donde se decretan las medidas que deben aplicarse con el fin de asegurar los bienes y la información federal de los Estados Unidos. La FISMA asigna al National Institute of Standard and Technology (NIST) la responsabilidad de desarrollar las normas y procedimientos de seguridad que las agencias gubernamentales americanas deben respetar con la meta de reforzar el nivel de seguridad de los sistemas de información. Estas normas se publicaron en el documento Federal Information Processing Standards Publication 200 (FIPS PUB 200) y se

describieron los controles de seguridad que deben efectuarse en el documento NIST Special Publication 800-53. Y es reportado al congreso anualmente por la oficina de Administración y Presupuesto (OMB, 2008).

Es notable el avance de los norteamericanos en la aplicación de las medidas decretadas por ley, habiendo logrado más del 93% de cumplimientos en materia de seguridad de la información federal como se puede apreciar en el siguiente cuadro:

Tabla 2 **Implementación de Sistemas de Seguridad de la Información en USA**

Percentage of Systems with a:	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008
Certification and Accreditation	47%	62%	77%	85%	88%	92%	96%
Tested Contingency Plan	35%	48%	57%	61%	77%	86%	92%
Tested Security Controls	60%	64%	76%	72%	88%	95%	93%
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304	10,679

Fuente: Oficina de Administración y Presupuesto (OMB, 2008).

En Europa, el gobierno del Reino Unido recomendó como parte de su Ley de Protección a la Información de 1998, que entró en vigencia el 1 de Marzo del 2000, que las compañías británicas utilicen BS 7799 como método para el cumplimiento de la ley (ASIMELEC, 2003).

En el mismo informe : “Estudio sobre el estado actual de la seguridad de los sistemas de la información en las empresas entrevistadas, de acuerdo con la Norma ISO/IEC17799:2000” realizado por Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), en la que se señala que fundamentado en la norma ISO desarrollada por un comité internacional y multidisciplinar de expertos, para que una organización tenga un buen nivel de seguridad, debería tener plenamente implantadas del orden del 90% de las recomendaciones (ASIMELEC, 2003).

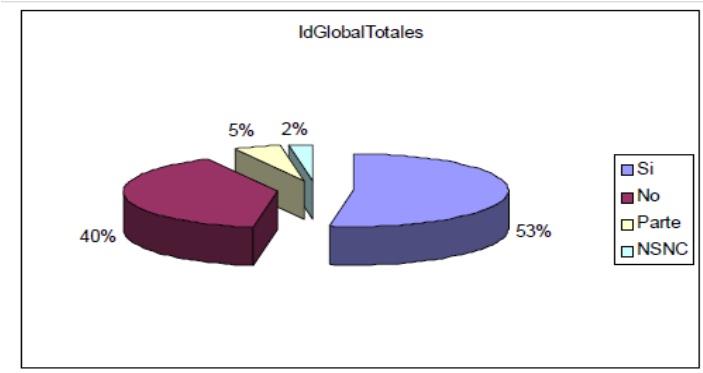

Grafico 4. **Nivel de implementación de SGSI ISO 17799 en España. (*Fuente* : informe ASIMELEC)**

Los resultados muestran que el grado de implantación de las recomendaciones de la norma son muy inferiores a lo que sería deseable. Desprendiéndose de ello como conclusión los siguientes puntos:

a) El mayor obstáculo a la implantación de la seguridad es la cultura empresarial, por encima de los problemas que a priori podrían parecer más relevantes como presupuesto o tecnología.

b) Las organizaciones consideran que un porcentaje muy elevado de las recomendaciones de seguridad no les son aplicables. Únicamente entre un 5% y un 10% de las recomendaciones pueden no ser aplicables en función de la naturaleza de la organización, por lo que realmente las respuestas de controles no aplicables, realmente reflejan problemas de desconocimiento, más que de no aplicabilidad.

c) El nivel de desconocimiento de los distintos aspectos que condicionan la seguridad es también más alto de lo que cabía esperar.

2.2.2 Latinoamérica

En México, en el 2008 el Departamento de Sistemas e Industrial de la Universidad del Valle de Atemajac (UNIVA) Campus Guadalajara, en coordinación con la Asociación Colombiana de Ingenieros en Sistemas

(ACIS), llevaron a cabo la Segunda Encuesta Nacional sobre Seguridad Informática en dicho país.

Los resultados del mencionado estudio en relación al uso de la norma ISO 17799/27001 en conjunto con otras normas de seguridad no supera el 47%, mientras que la norma certificable ISO 27001 alcanza un 26.1%.

En el mismo estudio se identifican los obstáculos para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) que reproducimos en la siguiente tabla:

Tabla 3 **Obstáculos para lograr un adecuado SGSI.**

OBSTÁCULOS PARA LOGRAR UN ADECUADO SGSI	2007	2008
Inexistencia de política de seguridad	22.2%	39.1%
Falta de tiempo	24.1%	52.2%
Falta de formación técnica	27.8%	30.4%
Falta de apoyo directivo	25.9%	26.1%
Falta de colaboración entre áreas/departamentos	29.6%	26.1%
Complejidad tecnológica	16.7%	17.4%
Poco entendimiento de la seguridad informática	16.7%	13.0%
Otros (Por favor especifique)	9.3%	13.0%

Fuente: **II Encuesta Nacional sobre Seguridad Informática en México, 2008**

De los resultados mostrados, se puede apreciar que los factores relacionados con la política, la dedicación a tiempo completo, la capacitación y el apoyo directivo son los mayores obstáculos para la implementación de los sistemas de seguridad en México.

2.2.3 Adopción e implementación de la ISO/IEC 17799 en el Perú

a) **La Agenda Digital Peruana**

Plan de Desarrollo de la Sociedad de la Información en el Perú, la Agenda Digital Peruana, ha sido desarrollado en el marco de la Comisión Multisectorial, formado por sector público, el sector privado y la sociedad civil para el Desarrollo de la Sociedad de la Información (CODESI), cuya creación se formaliza en junio de 2003, por Resolución Ministerial Nº 181-2003-PCM (CODESI, 2005).

En las siguientes líneas reproducimos el plan de acción de la Agenda que define la visión y los cinco objetivos estratégicos producto del trabajo de la comisión para cada uno de los principales ejes, bajo los cuales se desprenden las estrategias y acciones respectivas con miras a lograr el desarrollo de la Sociedad de la Información en el Perú

Visión: Sociedad basada en principios de equidad, integración y no discriminación que utiliza efectiva y eficientemente la información en sus procesos de desarrollo, a través del uso intensivo de las tecnologías de la información y comunicación.

Objetivo 1:Disponer de infraestructura de telecomunicaciones adecuada para el desarrollo de la Sociedad de la Información.

Objetivo 2:Promover el desarrollo de capacidades que permitan el acceso a la Sociedad de la Información.

Objetivo 3:Desarrollar el sector social del Perú garantizando el acceso a servicios sociales de calidad, promoviendo nuevas formas de trabajo digno, incentivando la investigación científica e innovación tecnológica, así como asegurando la inclusión social y el ejercicio pleno de la ciudadanía.

Objetivo 4:Realizar acciones de apoyo a los sectores de producción y de servicios en el desarrollo y aplicaciones de las TIC.

Objetivo 5:Acercar la administración del Estado y sus procesos a la ciudadanía y a las empresas en general, proveyendo servicios de

calidad, accesibles, seguros y oportunos, a través del uso intensivo de las TIC.(CODESI, 2005)

La CODESI, realiza por primera vez un diagnóstico y establece un conjunto de cinco objetivos estratégicos para permitir un desarrollo articulado y sostenido de la Sociedad de la Información en el país, el objetivo No 5 referido a Gobierno Electrónico, en la que se define la estrategia 5.1 del mismo, y entre las acciones correspondientes declara la acción No 6, como "Desarrollo de un plan de seguridad de la información para el sector público".

Considerando la importancia del Plan de seguridad de la información para el desarrollo del Proyecto de Gobierno Electrónico en el Perú, a propuesta de la ONGEI la PCM; a fin de homologar las iniciativas dentro del Sector, mediante Resolución Ministerial del 23 de Julio del año 2004 RM N°224-2004-PCM (2004**)**, decreta su aplicación y uso obligatorio en todas las instituciones Integrantes del Sistema Nacional de Informática y fijándose como plazo de dieciocho (18) meses para su implantación. En consecuencia, la implantación de la Norma Técnica Peruana debería haber finalizado en la totalidad de las instituciones en Enero del 2006. Sin embargo, el 8 de Noviembre del 2005 mediante una nueva Resolución Ministerial la RM No 395-2005-PCM (2005) se otorga una extensión de plazo cuya fecha límite sería el 30 de Junio del 2006.

Finalmente, 22 de agosto de 2007 del mismo modo que en los casos anteriores mediante resolución ministerial se aprobó la NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición" RM Nº 246-2007-PCM (2007), en reemplazo de la NTP-ISO/IEC17799:2004; manteniéndose el uso obligatorio de ésta segunda 2ªEdición, en todas las Entidades integrantes del Sistema Nacional de Informática, siendo ésta última una actualización de la norma.

La Norma Técnica Peruana está basada en la norma internacional ISO/IEC 17799 estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799, tiene su origen en la norma británica British Standard BS 7799-1 que fue publicada por primera vez en 1995 y va evolucionando continuamente como hemos indicado anteriormente. En la reseña histórica de la Norma Técnica Peruana versión 2007 literal (a.3) se lee textualmente RMNº 246-2007-PCM (2007):

> *Esta Norma Técnica Peruana es una adopción de la Norma ISO/IEC 17799:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.*

En adelante y durante el desarrollo de la presente investigación, nos referiremos a ella como la Norma o Norma Técnica Peruana en forma indistinta. En la VI Encuesta Nacional de Recursos Informáticos en la administración pública realizada por la ONGEI en el año 2007 se reporta:

> *De 576 Entidades Públicas sólo 124 (21,53%) instituciones públicas han iniciado el proceso de implementación de la Norma ISO 19977 – Buenas Prácticas en Seguridad de la Información, mientras que 78,47% aún no inician este proceso de implementación (VI ENRIAP, 2007 p.54).*

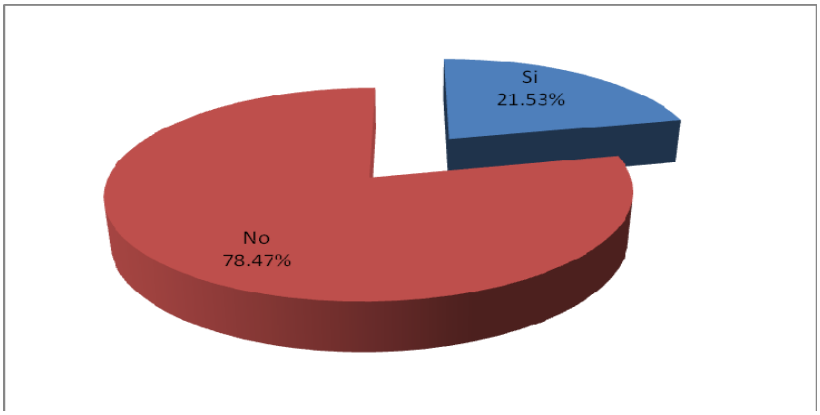

Grafico 5. **Porcentaje de procesos de implementación iniciados.**
Fuente: **VI ENRIAP 2007, ONGEI**

La norma ISO de seguridad de la información va evolucionado adaptándose a los nuevos escenarios que plantea la globalización, pues de acuerdo a la cronología de su historia que hemos ilustrado antes a la fecha se tiene la nueva serie ISO 27000, habiéndose publicado en el 2005 del estándar certificable ISO 27001, y el código de buenas prácticas ISO/IEC 17799 en el año 2007 ha sido reenumerado como la nueva ISO/IEC 27002 (ITGI, 2008 pág. 17).

En general en el Perú no se ha realizado estudios anteriores a la presente relativos a la adopción e implementación de los códigos de buenas prácticas de seguridad de la información, y su problemática, en el sector Público a excepción de los datos recogidos en la Encuesta Nacional de Recursos Informáticos y Tecnológicos de la Administración Pública realizada por la ONGEI (VI ENRIAP, 2007).

En el Sector Privado, encontramos una encuesta con el objetivo de determinar el nivel de aplicación de las Normas ISO 27001 y 27002 en las pequeñas y medianas empresas del departamento de Lambayeque por Msc Ing. Jessie Leila Bravo Jaico. Luego de analizar los resultados de la encuesta de cada uno de los dominios se expone que:

Dominio	No cumple	Cumple con excepciones	Si cumple
Todos los dominios	40%	42%	18%

Sólo el 18% de las empresas encuestadas cumplen con los 11 dominios de las Normas ISO 27000.

Aunque en los resultados de la encuesta no se hace finalmente una diferenciación entre las Normas ISO 27001 y 27002, consideramos como información puntual de referencia para nuestro caso.

2.2.4 Estructura de la Norma Técnica Peruana NTP-ISO/IEC 17799: 2007 EDI

La estructura de la NTP- ISO/IEC 17799:2007 ahora renombrado como la ISO 27002 es la siguiente (ISO, 2007)

16 Secciones:

0-4 Conceptos Generales (estas no aparecen en el cuadro)

11 Dominios de Seguridad

39 objetivos de control

133 Controles

Tabla 4. **Identificación de Dominios, Objetivos de control y Controles NTP- ISO/IEC 17799:2007**

Edición 2005		Objetivos	Controles
5	Política de Seguridad	1	2
6	Aspectos organizativos para la seguridad	2	11
7	Gestión de los activos	2	5
8	Seguridad de los Recursos Humanos	3	9
9	Seguridad física y del entorno	2	13
10	Gestión de comunicaciones y operaciones	10	32
11	Control de accesos	7	25
12	Adquisición, Desarrollo y mantenimiento de sistemas	6	16
13	Gestión de incidentes de seguridad de la información.	2	5
14	Gestión de continuidad del negocio	1	5
15	Conformidad	3	10
Totales		39	133

Fuente: **Construcción propia**

Los 11 dominios de la norma cubren la seguridad de la información en los cuatro aspectos: físicos, lógicos, organizacionales y legales como se puede apreciar en el siguiente gráfico.

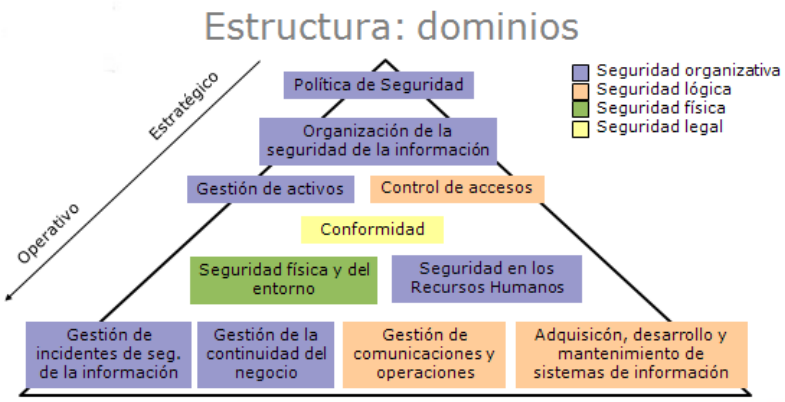

Grafico 6. **Estructura de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007**

Fuente: **Instituto Uruguayo de Normas Técnicas**

2.2.5 Factores críticos de éxito

De la revisión de la misma norma , se observa que se identifican como factores críticos de éxito los siguientes: a) Una política, objetivos y actividades que reflejen lo objetivos de negocio de la organización b) Un enfoque para implantar, mantener y monitorear e improvisar la seguridad que sea consistente con la cultura de la organización c) El apoyo visible y el compromiso de la alta gerencia d) La buena compresión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo e) La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados f) la distribución de guías sobre la política de seguridad de la información y de normas a todos los empleados y contratistas g) Aprovisionamiento para financiar actividades de gestión de la seguridad de la información h) la formación y capacitación adecuadas i) Establecer un efectivo proceso de gestión de incidentes de la seguridad de la información j) Un sistema integrado y equilibrado de medidas que permita evaluar el

rendimiento de la seguridad de la información y sugerir medidas (NTP 17799, 2005).

Uno de los puntos centrales de nuestra investigación será averiguar en qué medida los factores críticos de éxito antes mencionados han sido tomados en cuenta o no en el proceso de implementación por los principales actores del proceso.

Cada organización tiene una misión que describe la razón de su existencia (su propósito) y adonde quiere llegar (su Dirección). La misión refleja la singularidad de los valores y la visión. Llevar a cabo la misión compromete la participación y los conocimientos de toda la organización. Las metas y objetivos de cada miembro del equipo deberán estar orientados a cumplir la misión. Sin embargo lograr las metas y los objetivos no es suficiente. La organización deberá lograr un buen desempeño en actividades claves de forma consistente para cumplir con su misión. Estas áreas claves únicas para la organización y el sector en la que compite pueden ser definidos como los factores críticos de éxito de la organización.

Por lo tanto el método de los factores críticos de éxito es un medio para identificar estos importantes elementos que pueden ser definidos como los factores críticos de éxito de la organización (Caralli, 2004). Para la Gestión de la Seguridad de la Información como se ha mencionado anteriormente los factores críticos están identificados en la misma norma los cuales se enumeran en el punto correspondiente.

2.2.6 Resumen

La enorme capacidad para el procesamiento, almacenamiento, transporte y distribución de la información en todos los niveles y actividades de la sociedad es la evidencia de la presencia del fenómeno de la Sociedad de la Información. En nuestros tiempos La gran explosión del Internet, su ubicuidad, la masificación del uso de dispositivos móviles y la oferta libre y

democrática rica en servicios y contenidos a través de la red cambian drásticamente el comportamiento y los modos de interacción de los miembros de la sociedad con el estado, donde el intercambio del flujo de información de las organizaciones y los individuos se ven expuestos a las amenazas y peligros que atentan contra la confidencialidad, integridad y disponibilidad de la información, por tal motivo existe la imperiosa la necesidad de estandarizar los diversos proyectos y metodologías que se desarrollan en este campo a nivel global, como se ha podido establecer en el marco teórico el interés del estudio sobre la adopción e implementación de la norma internacional y el estado del arte de la seguridad de la información evoluciona alrededor de la norma internacional de Seguridad ISO 17799 y las series superiores (27000) correspondientes, respondiendo a la necesidad de consolidar la seguridad por el uso intensivo de Internet y las redes en las instituciones públicas.

También se puede apreciar que la adopción de la norma internacional está progresando sostenidamente a nivel mundial y regional principalmente en Europa, Asia y América del Norte, (Ernest&Young's, 2006), donde sobresalen España, Reino Unido, Japón y Estados Unidos, en Latino América sobresalen Brasil, Colombia y Chile, informaciones recogidas utilizando como herramienta principal las encuestas (ISO Survey, 2007), asimismo señalar que la estandarización de la norma también va acompañado por el desarrollo de las capacidades humanas especializadas cuya formación y certificación es administrada por importantes organismos independientes reconocidos Internacionalmente.

En nuestro país, las iniciativas sobre la adopción de la norma de seguridad de la información trata de seguir la tendencia internacional y se alinea con los objetivos estratégicos Nacionales de la Agenda Digital Peruana que marca el norte para las estrategias de desarrollo de la sociedad de la Información, entre los cuales el Gobierno Electrónico es la posibilidad más palpable para la socialización del uso de las TICs, dentro de un entorno favorable de seguridad y confianza. Por estas razones la PCM/ONGEI,

conscientes de los riesgos tecnológicos actuales, al cual están expuestos los activos de información de las diferentes organizaciones del sector público, y tomando en cuenta la contribución de la entidad rectora de la normalización como Indecopi decretó la obligatoriedad de la aplicación y uso de la Norma Técnica Peruana NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática con lo cual se ha institucionalizado la implementación de esta importante norma en el Perú bajo la responsabilidad de la ONGEI, para coadyuvar e impulsar el desarrollo del Gobierno Electrónico y la modernización del País.

En el siguiente capítulo trata sobre la metodología que se aplicará en nuestro estudio para la recolección, presentación y análisis correspondiente.

2.3 Definición de términos

TIC: Acrónimo de Tecnologías de Información y Comunicaciones

SI: Sociedad de la información, etapa de transición de la era Industrial

TCP/IP: Transport Control Protocol/ Internet Protocol

Internet: Es la interconexión descentralizada de redes de computadoras implementado en un conjunto de protocolos denominado TCP/IP

Gobierno electrónico: Consiste en el uso de las tecnologías de la información y el conocimiento en los procesos internos de gobierno y en la entrega de los productos y servicios del Estado tanto a los ciudadanos como a la industria.

Servicio en línea: Referidos a los servicios informativos y transaccionales que se ofrecen en una red abierta como Internet.

ISO: Es una Federación de organismos de normalización, con sede en Ginebra, formada por un solo representante por país.

IT (TI): Siglas del término en Inglés Information Technology

ONGEI: Oficina de Gobierno electrónico e Informática dependencia de la Presidencia de Consejo de Ministros encargada de Gobierno electrónico en el Perú.

Análisis de riesgo: Uso sistemático de la información para identificar fuentes y estimar riesgos.

SGSI: Sistema de Gestión de Seguridad de la Información.

Evaluación de riesgo: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.

Declaración de aplicabilidad (SOA): Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del SGSI.

IISP: Siglas en Inglés del Indtituto de Profesionales de Seguridad de la Información (Institute of Information Security Professionals).

CISSP: Siglas en Inglés de la Ceritifcación por IISP en Seguridad de la Información (Certified Information Systems Security Professional).

ISACA: Organismo Siglas en Inglés de La asociación de Auditoria de Sistemas de Información y Control.

CISM : Siglas en Inglés de la Certificación Otorgada por ISACA para administradores de Seguridad de la información (Certified Information Security Management)

CISA : Siglas en Inglés de la Certificación Otorgada por ISACA para auditores (Certified Information Systems Auditor).

CAPITULO III. METODOLOGÍA

3.1 Tipo de Investigación

La propuesta de investigación considera el empleo de una aproximación cuantitativa, transversal, con una estrategia basada en encuesta, usando el método de cuestionarios Semi-estructurado y un enfoque hipotético/deductivo.

La aplicación del cuestionario estará dirigido a los Directores o Gerentes de Sistemas de cada institución o de quienes hagan las veces como participantes en la implantación de la Norma Técnica Peruana NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en dichas entidades, usando como instrumento cuestionarios diseñados para tal fin. El trabajo de campo estará basado fundamentalmente en la realización de la encuesta y comprende el diseño, desarrollo, validación, distribución de la encuesta, y la recolección de la información obtenida para su correspondiente análisis.

A partir del análisis estadístico de las principales variables del problema objeto de la investigación se describirá y explicará las variables que condicionan los resultados obtenidos. Este conocimiento nos permitirá plantear las conclusiones y recomendaciones específicas para articular, orientar mejor las iniciativas y Proyectos de seguridad de la información dentro del sector , y por lo tanto; las inversiones realizadas, actuales y futuras por parte de las instituciones del Estado reviertan en beneficio de la implementación más acelerada y efectiva de los sistemas de Gestión de la Seguridad de la información para impulsar el desarrollo del Gobierno Electrónico en el Perú, la modernización del estado, generar confianza en

los sistemas de información administrados por el estado y consecuentemente la mejora en la calidad de los servicios públicos.

Se utilizará una adaptación del diseño de la encuesta de la consultora Americana WolcottGroup (2007) como enfoque genérico, aplicando para ello la norma ISO 17799 – 2005 como parte de los elementos a ser evaluados. Se aplicaran como herramienta de recolección de información la encuesta a todos los organismos Públicos Descentralizados Adscritos a la PCM en total 16 Instituciones con Sede en la ciudad de Lima.

El diseño preliminar de la encuesta fue adaptada por el investigador y propuesta a la ONGEI, revisada por la ONGEI , validada en reuniones posteriores que incluyó el documento de comunicación (Oficio) propuesto y finalmente aprobada. Actualmente se encuentra en proceso de Recolección de datos.

3.2 Modelo de Investigación

La revisión de la literatura diversos autores consideran que para una implementación exitosa del Sistema de Gestión de Seguridad de la Información (SGSI) debe tenerse en cuenta el factor humano, la seguridad de la información es un problema más que nada de dirección que tiene algunas soluciones tecnológicas (Whitman y Caylor, 2005, p.105) , la convicción y la declaración de la necesidad son muy importantes para estimar esfuerzos y costos para futuros planes (Al-Hamdani Wasim A, 2006, p 106), siendo así que estos aspectos fundamentan la adopción e implementación de un sistema de gestión de Seguridad de la información en una organización.

Por otra parte, el emprendimiento en el proceso de planificación y alineamiento de la seguridad de la información con los objetivos estratégicos institucionales, resulta crítico para la organización (Partida, Ezingerad, 2007); de allí que el enfoque y la gestión del proceso resultan vitales para materializar al aplicación de la norma, sobre la cual se soporte el grado de madurez que se pueda alcanzar en su implementación.

También se ha encontrado en la literatura abundante material de diversos autores sobre la influencia de los factores críticos de éxito en el grado de madurez y el éxito en la implementación de un SGSI.

La siguiente tabla muestra la relación de los factores críticos de éxito fundamentales del modelo extraído del marco teórico.

Tabla 5. **Factores Críticos de Éxito**

Ítem	Descripción	**Revisión de Literatura**
1	Una política, que refleje los objetivos de la organización	(ISO 27002, 2005), (Hafez Amer, Hamilton, Jr., 2008), (Jinx P. Walton, 2002), (Preda, Cuppens, boulahia, alfaro, toutain, Elrakaiby, 2009), (NIST, 2006)
2	El apoyo visible y el compromiso de la alta gerencia	(ISO 27002, 2005), (Jan Yestingsmeier & Steve Guynes, 1982),(NIST, 2006), (Alfawaz, May y Mohanak, 2008)
3	La convicción de la necesidad de la seguridad	(ISO 27002, 2005), (Jan Yestingsmeier & Steve Guynes, 1982), (Spears, 2006), (NIST,2006)
4	Difusión de la política de seguridad	(ISO 27002, 2005), (Jinx P. Walton, 2002),), (Preda, Cuppens, boulahia, alfaro, toutain, Elrakaiby, 2009)
5	Financiamiento para la gestión de la seguridad de la información	(ISO 27002, 2005),(R. Conkling, "Drew" Hamilton, 2008) (Lawrence a. Gordon, Martin p. Loeb, 2002), (Fumey-Nassah, 2007)
6	implantación consistente con la cultura de la organización	(ISO 27002, 2005),(Stallings, 2007), (Hafez Amer, Hamilton, Jr., 2008), (Koskosas, Ray J. Paul, 2004), (Alfawaz, May y Mohanak, 2008)
7	Requisitos de la seguridad, evaluación y gestión del riesgo	(ISO 27002, 2005),(Koskosas, Ray J. Paul, 2004), (Rodewald, 2005), (NIST, 2006)
8	Formación y capacitación adecuadas	(ISO 27002, 2005),(Al-Hamdani, 2006), (ENISA, 2008), (Alfawaz, May y Mohanak, 2008)
9	Gestión de incidentes de la seguridad de la información	(ISO 27002, 2005),(Rollason-Reese, 2003), (Farahmand, Navathe, Sharp, Enslow, 2003), (NIST, 2006)
10	Métricas para evaluar el rendimiento de la seguridad de la información	(ISO 27002, 2005),(An Wang, 2005),(Savola,2007), (NIST, 2006)

En base a estas consideraciones se definen las variables para la investigación.

3.2.1 Variables del Estudio

Conceptualmente definimos para el estudio 03 variables independientes:

a) Nivel de valoración de la Norma por la Institución

b) Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma

c) Influencia de los Factores Críticos en la implementación de la Norma.

d) el grado de madurez alcanzado en la implementación.

Las variables se han operacionalizado identificando sus dimensiones y sub dimensiones según corresponda, los indicadores y una escala de medición los cuales se presenta en la Tabla de Operacionalización de las mismas.

En la siguiente figura se esquematiza el modelo de la investigación:

MODELO DE INVESTIGACIÓN

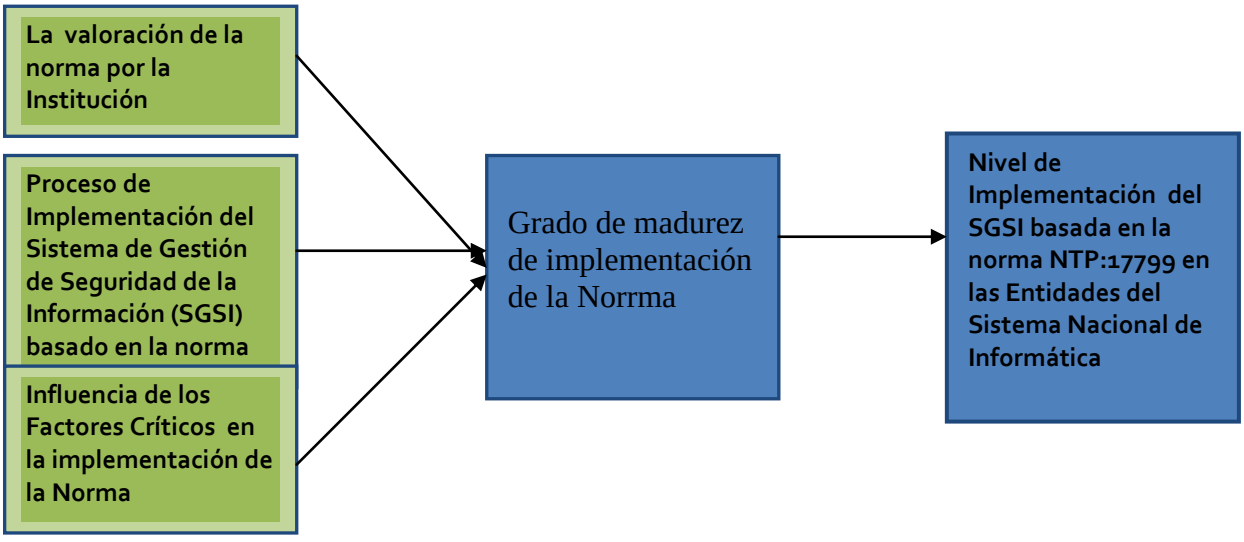

Grafico 7. **Modelo de Investigación. Fuente: Elaboración Investigador**

3.2.2 Descripción del modelo

El modelo relaciona las variables independientes con la variable dependiente el cual determina el grado de madurez de la Implementación de la Norma, con lo que se podrá conocer el nivel de implementación alcanzado en las Instituciones objeto del estudio.

Con las variables se ha definido dimensiones y sub dimensiones, y una escala de medición que permitirá recopilar información con suficiente detalle sobre las variables: Valoración de la Norma por la Institución, el proceso de implementación, los factores críticos de éxito, factores que en forma global influyen en el grado de madurez alcanzada.

a) El Nivel de valoración de la Norma por parte de la Institución**,** esta variable medirá la importancia que se le ha dado a la norma, conocimiento alcanzado y la potencialidad para aportar beneficios a la organización. Este aspecto es de mucha importancia para ver si es una barrera para la adopción como código las buenas prácticas de Seguridad de la Información.

b) Proceso de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma**,** permitirá indagar el nivel de dificultad en el enfoque, la planificación, uso de metodologías para: definición de requisitos, procesos, evaluación y tratamiento de los riesgos; controles seleccionados, la Declaración de Aplicabilidad que permita evidenciar el avance en el logro de los objetivos para una implantación exitosa de un Sistema de Gestión de Seguridad de la Información en la organización.

c) Grado de Influencia de los factores críticos en la implementación de la Norma**,** nos indicará en qué medida se han identificado y

tomado en cuenta los factores críticos de éxito en el proceso de implementación de la Norma. Estos factores son abordados en la literatura desde diferentes puntos de vista por los diferentes autores y son considerados críticos para una implementación exitosa del Sistema de Gestión de Seguridad de la Información.

d) Grado de Madurez de la Implementación de la Norma**,** valora los logros alcanzados en la implementación de la norma en las diferentes dimensiones que se ha definido para la variable, como está especificada en la tabla de operacionalización de la misma reflejando la influencia de los variables de las que depende.

3.3 Hipótesis de la Investigación

En general como consecuencia de los pasos previos dados dentro de la investigación, existen razones para afirmar que existen factores que inhiben e influyen en el bajo nivel de implantación que ha alcanzado la Norma Técnica NTP-ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática, en esta sección se desarrollan las hipótesis en concordancia con el modelo diseñado:

a) Sobre el Nivel de valoración de la Norma por parte de la Institución
H1: No hay la convicción suficiente de que la norma NTP de Seguridad de la Información agregue valor para la Institución por parte de los responsables de la implementación.

b) Proceso de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma.

H2: La Mayoría de las instituciones adscritas a la PCM no han iniciado el proceso de Implementación de la Norma de Seguridad de la Información, lo cual contribuye al atraso en la implementación en la administración pública.

H2.1: El compromiso de la alta dirección, influye positivamente en el proceso de inicio y sostenimiento de la implementación de la NTP 17799, en los Organismos Descentralizados Adscritos a la PCM.

H2.2: La elección de una metodología para la gestión y evaluación de riesgos de los activos críticos facilita el encaminamiento del desarrollo del proceso de implementación de la norma.

H2.3: Existe alto grado de dificultad en las cuatro etapas de implementación que contempla el modelo simplificado definido por la ONGEI, lo cual dificulta el avance en la implementación de la norma NTP 17799

H2.4: La falta de personal especializado y capacitación del personal dentro de las instituciones, influye negativamente en la implementación de la norma.

H2.5: Existen dificultades en la gestión del proyecto y obtener resultados esperados debido a la falta de una cultura organizacional orientado a la seguridad de la información.

c) Grado de Influencia de los factores críticos en la implementación de la Norma,

H3: El grado de influencia de los factores críticos es percibido como alta por los responsables de la implementación de la Norma lo cual influye positivamente en la implementación de la norma.

H3.1: La formalización del Área de Seguridad, la cultura organizacional, el apoyo de la alta dirección y personal especializado tienen una alta influencia en la implementación exitosa de la Norma.

d) Grado de Madurez de la Implementación de la Norma.

H.4 El nivel de madurez de la implementación de la norma se encuentra en la etapa inicial.

3.4 Diseño de la investigación

3.4.1 Población Objetivo

Está constituido por las instituciones que conforma las Entidades del Sistema Nacional de Informática del Estado dentro del cual está inmersa la muestra elegida constituida por los Organismos Públicos Descentralizados Adscritos a la Presidencia del Consejo de Ministros del Gobierno Nacional.

3.4.2 Características de la Población

El Sistema Nacional de Informática, fue creado por Decreto Legislativo N° 604, con el fin de organizar las actividades y proyectos que en materia de informática realiza las instituciones públicas del Estado, así como su relación con otros sistemas y áreas de la Administración Pública (www.ongei.gob.pe).

Miembros que conforman el Sistema Nacional de Informática:

1. El Consejo Consultivo Nacional de Informática (CCNI)
2. El Comité de Coordinación Interinstitucional de Informática (CCII)
3. Las Oficinas Sectoriales de Informática y demás Oficinas de Informática de los Ministerios, de los Organismos Centrales, Organismos Públicos Descentralizadas y Empresas del Estado
4. Los Órganos de Informática de las Municipalidades
5. Los Órganos de Informática de los Poderes Públicos y de los Organismos Autónomos.

Los Organismos Públicos Descentralizados adscritos a la PCM, forman parte del conjunto de Entidades del Sistema Nacional de Informática, están representados por el Titular de la Institución y tienen dentro de su estructura organizativa las oficinas de Informática (Directorio ODP) que son indistintamente denominadas como Gerencia, Dirección o Área.

El siguiente cuadro obtenido de la página web de la PCM ilustra la conformación de los organismos mencionados y sus respectivos titulares:

Tabla 6. **Organismos Públicos Descentralizados adscritos a la PCM**

Despacho Presidencial (DP)- Secretario General: Luis Nava Guibert Telf: 311-3900 www.presidencia.gob.pe
Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA) Presidente Ejecutivo: Romulo Pizarro Tomasio Telf: 449-0007 www.devida.gob.pe
Dirección Nacional de Inteligencia (DINI) Director Ejecutivo: Danilo Apolonio Guevara Zegarra Telf: 213-5165 www.dini.gob.pe
Instituto Nacional de Defensa Civil (INDECI) Jefe: Luis Palomino Rodríguez Telf: 225-9898 www.indeci.gob.pe
Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) Presidente del Directorio: Jaime Thorne León Telf: 224-7800 www.indecopi.gob.pe
Instituto Nacional de Estadística e Informática de Perú (INEI) Jefe: Renán Quispe Llanos Telf: 433-4223 www.inei.gob.pe
Instituto Nacional de Radio y Televisión Peruana (IRTP) Presidente Ejecutivo: C. Alberto Manrique Negron Telf: 619-0707 www.tnp.com.pe
Cuerpo General de Bomberos Voluntarios del Perú (CGBVP) Comandante General: Roberto Ognio Baluarte Telf: 222-0222 www.bomberosperu.gob.pe
Sierra Exportadora Presidente Ejecutivo: Gastón Benza PFlucker Telf: 215-0730 www.sierraexportadora.gob.pe
Centro Nacional de Planeamiento Estratégico (CEPLAN)

Presidente del Consejo Directivo: Agustín Haya de la Torre de la Rosa Telf: 628-7285 http://www.ceplan.gob.pe
Autoridad Nacional del Servicio Civil (SERVIR) Presidenta Ejecutiva:Nuria Esparch Fernández Telf: 421-3383 http://www.servir.gob.pe
Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre (OSINFOR) Telf: 421-9018 www.osinfor.gob.pe
Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN) www.osinergmin.gob.pe
Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL) www.osinergmin.gob.pe
Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (OSITRAN) www.osinergmin.gob.pe
Superintendencia Nacional de Servicios de Saneamiento (SUNASS) www.osinergmin.gob.pe

***Fuente*. Portal del Estado Peruano**

Los organismos conformantes del cuadro No 6 cuentan con una oficina o Unidad informática encargada de la gestión de las Tecnologías de la Información y de la Seguridad de la información.

La Presidencia del Consejo de Ministros (PCM), es un organismo técnico - administrativo normado por la Ley del Poder Ejecutivo, cuya máxima autoridad es el Presidente del Consejo de Ministros, Los organismos públicos descentralizados forman parte de la estructura organizativa de la PCM el cual se encuentra definido en el Reglamento de Organización y Funciones, documento normativo de gestión institucional que formaliza la estructura orgánica de la Entidad, conteniendo las funciones generales de la Entidad y las funciones específicas de los órganos y unidades orgánicas y establece sus relaciones y responsabilidades DS Nº 063-2007-PCM (2007). , se presenta el siguiente organigrama en la cual la línea roja interrumpida

encierra los la posición en el organigrama de la PCM de los organismos Públicos objeto del estudio.

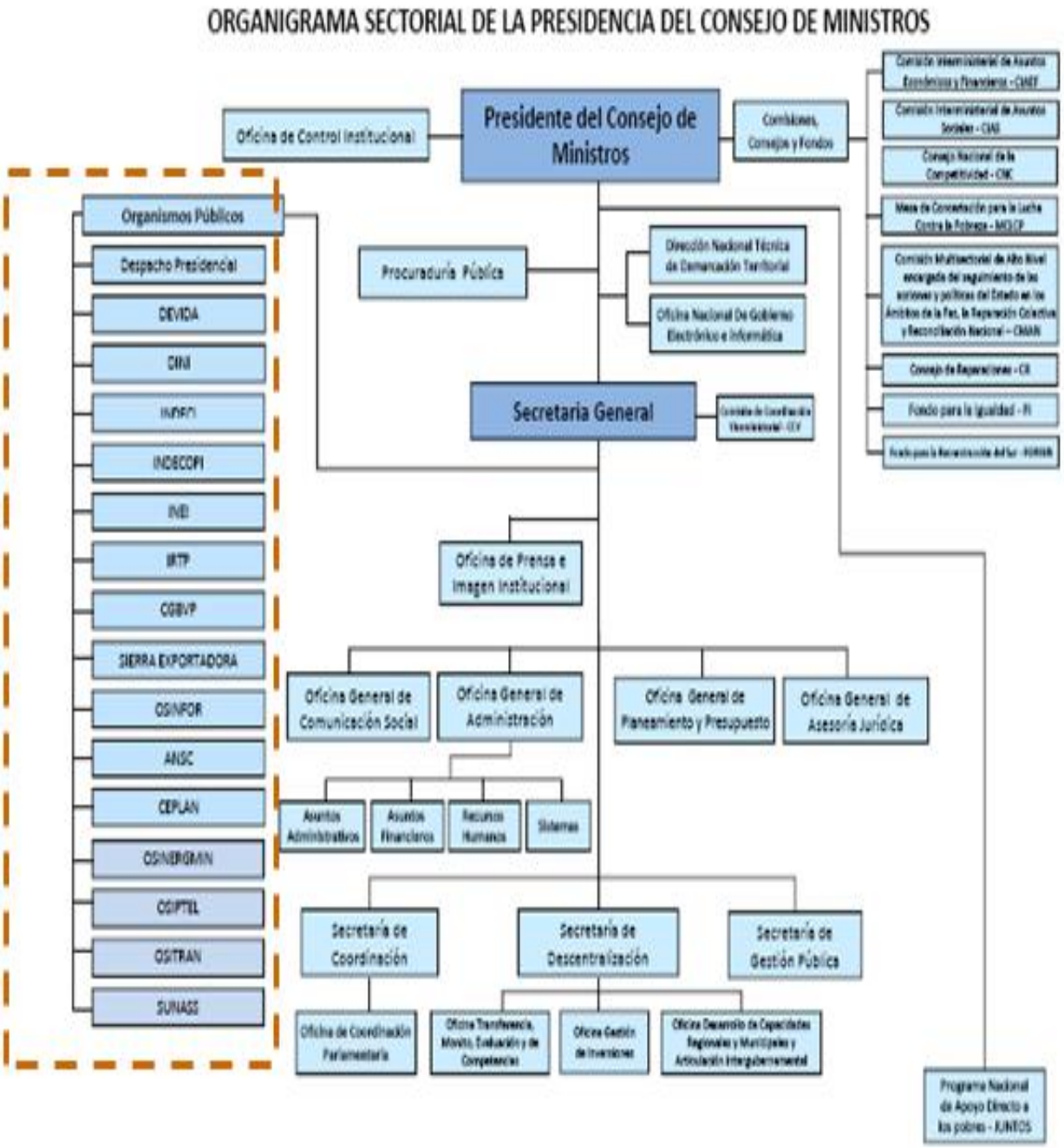

Grafico 8. **Organigrama de la PCM**

***Fuente*. Portal PCM**

Tabla 7 **Directorio de las unidades de informática de los Organismos Descentralizados adscritos a la PCM**

***Fuente*: Elaborado por el investigador**

No	Institución	Responsable	Cargo	Nobre de la Unidad Informática	E-mail	Dirección	Ubicación
1	Despacho Presidencial	OSCAR ALDO QUISPE SANTA MARIA	Director	Dirección de Tecnologías de la Información y Sistemas	aquispe@presidencia.gob.pe	Jr. De la Unión 1ra. Cdra. S/N - Casa de Gobierno	Lima
2	Comisión Nacional para el Desarrollo y Vida sin Drogas - DEVIDA	CARLOS WILFREDO PAREDES ZUÑIGA	Gerente	Gerencia de Administración e Informática	cparedes@devida.gob.pe	Av. Benavides 2199-B	Miraflores
3	Instituto Nacional de Defensa Civil - INDECI	LUIS MALDONADO GONZALEZ	Jefe	Oficina de Estadistica y Telemática	lmaldonado@indeci.gob.pe	Esquina Calles 1 y 21. Urb. Córpac	San Isidro
4	Instituto Nacional de Radio y Televisión del Perú	WILFREDO CASTRO CABANILLAS	Jefe	Oficina de Informática y Estadística	wcastro@tvperu.gob.pe	José Gálvez 1040 Santa Beatriz	Lima
5	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI	VICTOR PACHECO POSTIGO	Gerente	Oficina de Informática y Sistemas	vpacheco@indecopi.gob.pe	Calle La Prosa 138	San Borja
6	Instituto Nacional de Estadística e Informática - INEI	DANIEL MAGUIÑA HUERTA	Director Técnico	Director Técnico de Informática	daniel.maguina@Inei.gob.pe	Av. General Garzón 658	Jesús María
7	Dirección Nacional de Inteligencia Estratégica - DINI	CESAR BERROCAL DEL AGUILA	Jefe	Oficina de Soporte Técnico	of402@dini.gob.pe	Av Edmundo Aguilar S/N exAv. Las palmas	Barranco
8	Cuerpo General de Bomberos Voluntarios del Perú	JAVIER ERKEN BOSSMAN	Director	Dirección de Informática	jerken@bomberosperu.gob.pe	Av. Salaverry 2495	San Isidro
9	Organismo Supervisor de Inversión Privada en Telecomunicaciones	AUGUSTO MORA OBREGON	Jefe	Oficina de Informática y Sistemas	amora@osiptel.gob.pe	Calle La Prosa 136	San Borja
10	Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público - OSITRAN	EDUARDO MORAN HUANAY	Jefe	Jefe de Desarrollo Institucional y Sistemas	emoran@ositran.gob.pe	Av. República de Panamá 3659 Urb. El Palomar	San Isidro
11	Organismo Supervisor de la Inversión Privada en Energía	JULIO PUERTAS VILLAR	Jefe	Oficina de Informática	jpuertas@osinerg.gob.pe	Bernardo Monteagudo 222	Magdalena del Mar
12	Superintendencia Nacional de Servicios de Saneamiento - SUNASS	CESAR GAMARRA MALCA	Jefe	Oficina de Sistemas	cgamarra@sunass.gob.pe	Av. Bernado Monteagudo 210-216	Magdalena del Mar
13	Planeamiento Estratégico (CEPLAN	CARLOS LOAIZA SELIM	Jefe	Oficina General de Administración	cloaiza@ceplan.gob.pe	Av. Canaval y Moreyra 150 piso	San Isidro
14	Sierra Exportadora	IVAN MONGE VALENZUELA	Jefe	Unidad de Tecnologias de Informacion	imonge@sierraexportadora.gob.pe	Avenida Conquistadores N° 970	San Isidro
15	Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR	ROEL ORELLANA SANCHEZ	encargado	Oficina de informatica	rorellana@osinfor.gob.pe	Paseo de la Republica Nro. 3147, Of.301	San Isidro
16	Autoridad Nacional del Servicio Civil - SERVIR	ALEJANDRO ALFONSO REA MORALES	Jefe	Oficina de Tecnologias de la Información y Comunicaciones	area@servir.gob.pe	Calle Manuel Gonzáles Olaechea 448	San Isidro

3.5 Consentimiento Informado

La información restringida por su naturaleza y que se use en el presente estudio contará con las autorizaciones respectivas de los propietarios de la información.

3.6 Marco Muestral

3.6.1 Población

Como se ha mencionado en el apartado anterior, la población comprende a todas la Entidades del Sistema Nacional de Informática del Estado Peruano. La muestra posee un carácter intencionado y no probabilístico estableciéndose como muestra a los todos los Organismos Públicos Descentralizados adscritas a la Presidencia del Consejo de Ministros PCM del Gobierno y que tienen su Sede en la ciudad de Lima conformado por 16 Instituciones.

La razones principales del tipo de muestra elegida son: a) El investigador trabaja en una de las instituciones adscritas a la PCM, por lo que existen condiciones favorables para la recopilación de la información b) La Presidencia del Consejo de Ministros (PCM) actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), que ha emitido las Resoluciones Ministeriales para la implementación obligatoria de la norma en todas las Entidades integrantes del Sistema Nacional de Informática. c) La ONGEI tiene interés en los resultados de la investigación respecto a las dificultades que enfrentan en la implementación de la Norma los organismos incluidos en la investigación.

3.6.2 Relevancia de las organizaciones de la muestra

Los Organismos Públicos Descentralizados Adscritas a la Presidencia del Consejo de Ministros PCM , forman parte de un grupo de entidades desconcentradas del Poder Ejecutivo, con personería jurídica de Derecho Público. Tienen competencias de alcance nacional (Ley Orgánica del Poder Ejecutivo Ley nº 29158, título IV).

Dichos organismos dependen de la más alta autoridad de la Presidencia del Consejo de Ministros y realizan funciones económicas y reguladoras primordiales del Estado que tienen gran importancia y un rol protagónico dentro de la estrategia del proceso de modernización del país.

Los organismos públicos adscritos a la PCM incursos en este estudio pertenecen y reciben la calificación de la máxima instancia del gobierno nacional como Organismos Ejecutores, Organismos Especializados; y dentro de esta última categoría se encuentran los Organismos Técnicos Especializados y los Organismos Reguladores.

En todos los casos, estos organismos ejercen funciones de prestación de servicios, planificación, supervisión, o ejecución y control de las políticas de Estado de largo plazo según su competencia, y es de carácter multisectorial, de ámbito nacional o intergubernamental (ver anexo 5. Funciones de los Organismos Públicos Descentralizados adscritos a la PCM).

3.7 Unidad de Análisis

Nuestra unidad de Análisis comprende a todos los Directores, Gerentes o quienes hagan las veces de los 16 Organismos Públicos Descentralizados, que participan en la implementación de un sistema de Gestión de Seguridad de la Información basada en la Norma Técnica Peruana NTP-ISO/IEC 17799.

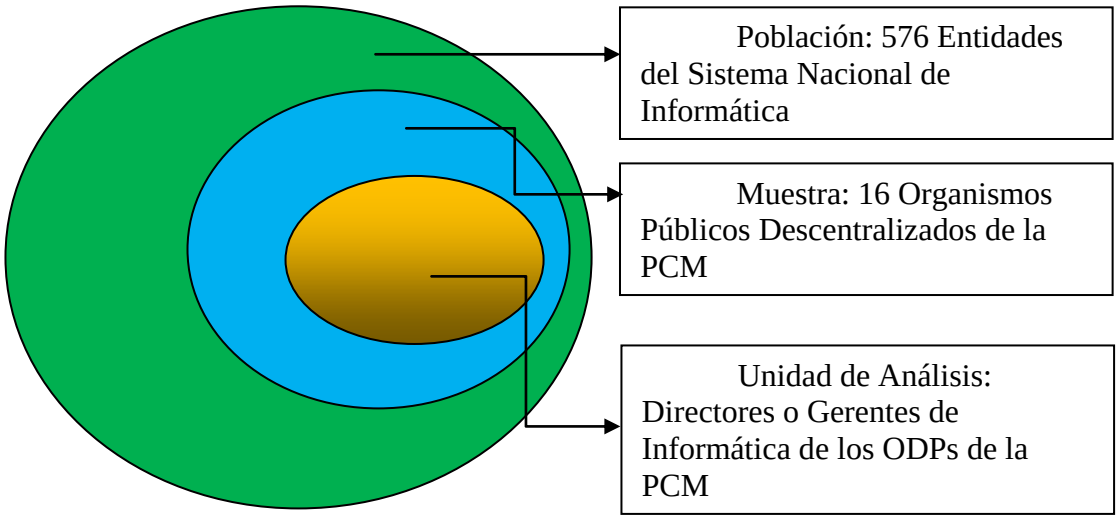

Grafico 9. **Diagrama de Población, muestra y unidad de Análisis**

Fuente: Elaboración del Investigador

3.8 Confidencialidad

Se garantiza la confidencialidad de información sensible de acuerdo a la legislación vigente.

3.9 Localización Geográfica

El desarrollo de la investigación se realizara en las Entidades del Sistema Nacional de Informática del Estado, Sector de Gobierno Nacional y adscritas a la Presidencia del Consejo de Ministros PCM y que tienen su Sede en la ciudad de Lima.

3.10 Conformidad del Diseño

El diseño de la investigación es conforme con las metodologías más usadas en el campo académico y científico el cual nos permitirá capturar los datos primarios mediante el uso de encuestas al personal clave de la unidad de análisis con lo cual se tendrá los insumos necesarios para el análisis de la información recopilada a fin lograr los objetivos de la Investigación.

3.11 Instrumentación

La presente de investigación con enfoque cuantitativo descriptivo utilizará una encuesta en la unidad de análisis, a través de un cuestionario como instrumento principal, para la recolección de información primaria previa operacionalización de las variables independientes y dependientes definidas para el estudio (Ver Anexo 3).

Es necesario indicar, dado que la investigación enfoca una problema dentro del ámbito de la administración pública, en el marco del programa de modernización del estado y la Agenda Digital Peruana; siendo la implementación de la Norma de Seguridad, un componente crítico del proyecto de Gobierno Electrónico que la Oficina de Gobierno Electrónico e Informática (ONGEI) viene impulsando a nivel de las Entidades del Sistema Nacional de Informática del Estado Peruano (RM-246-2007-PCM, 2007), el investigador realizó coordinaciones con el jefe de dicha oficina y el personal responsable de la Gestión de la Seguridad de la información de dicha oficina, que ha mostrado interés en la realización de la investigación por ser de relevancia en el ámbito del sector. y viene apoyando la realización de la encuesta en la unidad de análisis elegida para la presente investigación.

3.11.1 Operacionalización de las Variables. La tabla que desarrolla la operacionalización de las 04 variables, con sus respectivas dimensiones y subdimensiones definidas para la investigación se encuentra en el anexo 5 del presente estudio.

La siguiente tabla obtenida de la operacionalización de las variables relaciona las variables y el cuestionario para la prueba de hipótesis:

Tabla 8. **Tabla de relación de variables, hipótesis y preguntas de la encuesta: Elaboración del Investigador**

Variable	Factor	Hipótesis	Pregunta de la encuesta
a) El Nivel de valoración de la Norma por parte de la Institución	Política de Seguridad	H1	Parte I: Dominio 1:Pregunta 1,2, 3
	Organización de la Seguridad de la Información		Parte I: Dominio 2:Pregunta 1,2, 3
	Gestión de Activos		Parte I: Dominio 3:Pregunta 1,2, 3
	Seguridad de Recursos Humanos		Parte I: Dominio 4:Pregunta 1,2
	Seguridad física y ambiental		Parte I: Dominio 5:Pregunta 1
	Gestión de las comunicaciones y operaciones		Parte I: Dominio 6:Pregunta 1,2
	Control de Acceso		Parte I: Dominio 7:Pregunta 1
	Adquisición, desarrollo y Mant. De sistemas de información		Parte I: Dominio 8:Pregunta 1,2
	Gestión de incidencias		Parte I: Dominio 9:Pregunta 1
	Gestión de Continuidad del Negocio		Parte I: Dominio 10:Pregunta 1
	Cumplimiento		Parte I: Dominio 11:Pregunta 1
b) Proceso de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma NTP	Iniciación de Proceso	H2 H2.1 H2.2	Parte II: Pregunta 1
	Elección de Metodología	H2.3	Parte II: Pregunta 2
	Definición de alcance	H2.4 Y	Parte II: Pregnta 3
	Aplicación de la Norma	H2.5	Parte II: Pregunta 4 y5
	Plan de Implementación Etapal, II, III y IV		
	Otros factores que dificultan		Parte II: Pregunta 6

	Responsabilidad de la Seguridad de la Información		Parte II: Pregunta 7
	Medidas para fomentar cumplimiento de la Norma		Parte II: Pregunta 8
c). Grado de Influencia de los factores críticos en la implementación de la Norma,	Personal Especializado	H3 H3.1	Parte III: Pregunta 1,2 y 3
	Presupuesto		
	Entendimiento sobre seguridad de la información Alta Dirección		
	Concienciación y Capacitación		
	Alineamiento de la seguridad con los objetivos estratégicos		
	Gestión del Proyecto		
	Formalización del area de Seguridad		
	Cultura organizacional		
d) El Nivel de Madurez de la implementación de la norma por parte de la Institución	Política de Seguridad	H4	Parte I: Dominio 1:Pregunta 1,2, 3
	Organización de la Seguridad de la Información		Parte I: Dominio 2:Pregunta 1,2, 3
	Gestión de Activos		Parte I: Dominio 3:Pregunta 1,2, 3
	Seguridad de Recursos Humanos		Parte I: Dominio 4:Pregunta 1,2
	Seguridad física y ambiental		Parte I: Dominio 5:Pregunta 1
	Gestión de las comunicaciones y operaciones		Parte I: Dominio 6:Pregunta 1,2
	Control de Acceso		Parte I: Dominio 7:Pregunta 1

	Adquisición, desarrollo y Mant. De sistemas de información		Parte I: Dominio 8:Pregunta 1,2
	Gestión de incidencias		Parte I: Dominio 9:Pregunta 1
	Gestión de Continuidad del Negocio		Parte I: Dominio 10:Pregunta 1
	Cumplimiento		Parte I: Dominio 11:Pregunta 1

Se ha llevado a cabo el siguiente procedimiento en el diseño de la encuesta, para llevar a cabo la recolección de datos mediante la encuesta:

a) Durante el proceso de investigación y revisión de literatura se identificó una encuesta relacionada con el tema, de acceso público en la página WEB de la Consultora Americana WolcottGroup, que luego de su revisión fue traducida al español (Certificada).

b) Elaboración de la encuesta, como se mencionó anteriormente es una adaptación de la encuesta de la Consultora WolcottGroup que cubre la parte I de la misma, se amplió el enfoque para la parte II y III, rediseñándose las preguntas del cuestionario de acuerdo al modelo de investigación planteado, el cuestionario completo de la encuesta se pude verificar en el Anexo 2, del presente estudio.

c) La Encuesta fue revisada y mejorada con la colaboración de 03 especialistas: Un profesional experto con experiencia en la implementación de la Norma NTP ISO/IEC 17799 y logrado la certificación respectiva en la ONPE, el responsable de la implantación de la norma en OSIPTEL, y un consultor de Seguridad de la Información de una empresa privada con experiencia en la Norma NTP ISO/IEC 17799, quienes se participaron en la prueba de ejecución de la encuesta.

d) Con la propuesta de la encuesta final, se realizó coordinaciones para una reunión con el jefe de la ONGEI y el responsable de Seguridad de la Información del Programa de Gobierno Electrónico para su validación.

En posteriores coordinaciones con ONGEI se estableció que la estrategia más conveniente de acuerdo a la cultura estatal era remitir la encuesta mediante un oficio múltiple firmada por la máxima autoridad de la ONGEI a los Directores o Gerentes de las Oficinas de Informática de los Organismos Descentralizados Adscritos a la PCM

e) Revisión y Aprobación, la encuesta y el modelo de oficio para remitir a los organismos fue revisada y aprobada por el Jefe de la ONGEI.

f) Comunicación de la encuesta, esta fue remitida como oficio múltiple No. 034-2009/PCM el 1 de setiembre de 2009 a los 16 directores o Gerentes de Sistemas de Información de la unidad de análisis.

g) Seguimiento, mediante llamadas telefónicas y correo electrónico

h) Recepción de la encuesta, la recepción de las encuesta se realiza en las oficinas de Seguridad de la Información de la ONGEI. Documentos que fueron entregados al investigador para su procesamiento.

i) Verificación de la encuesta.
j) Tabulación
k) Revisión de la tabulación en Hoja Excel
l) Estadística descriptiva
m) Análisis e interpretación
n) Conclusiones y recomendaciones

3.12 Colección de la Data

3.12.1 Resultados de la recolección de datos

El método de recopilación de datos para esta investigación se ha realizado aplicando una encuesta a la unidad de análisis mediante un cuestionario de tipo Semi estructurado. El investigador ha diseñado un cuestionario que comprende un conjunto de preguntas que cubren los

aspectos (variables) más relevantes respecto a la valoración(adopción), proceso de implantación de la NTP: 17799 y los factores críticos de éxito, además del nivel de madurez alcanzado por las instituciones que permitió recoger información necesaria para validar las hipótesis del estudio.

La encuesta tiene 3 Partes:

I. Sobre la valoración, el grado de madurez en la implementación de los Dominios de Control de la Norma Técnica Peruana NTP-ISO/IEC 17799: 20 Preguntas
II. Sobre el Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información basado en la Norma: 8 Preguntas
III. Sobre el grado de influencia de los Factores Críticos en la implementación de la Norma: 3 Preguntas

La encuesta fue remitida mediante oficio múltiple 0034-2009-PCM/ONGEI del 01 de Setiembre 2009, por el jefe de la Oficina Nacional de Gobierno Electrónico ONGEI a los 16 Directores, Gerentes o jefes de Informática que conforman Organismos Públicos Descentralizados adscritos a la PCM, La encuesta fue respondida por el 100% de la unidad de análisis.

Durante la etapa de revisión y tabulación de la encuesta se detectó errores en las respuestas a la Pregunta Nº 6 Parte II del cuestionario por parte de 11 participantes de la Unidad de Análisis que ameritó una coordinación aclaratoria con cada uno de ellos vía telefónica remitiéndoseles luego nuevamente el formato correspondiente a la pregunta mencionada por correo electrónico. La cual fue completada por los 11 participantes al 4 de Febrero del 2010.

Total de respuestas recibidas:

Respondieron la encuesta en su totalidad las 16 Instituciones conformantes de la unidad de análisis. El medio para la entrega fue mediante Oficio dirigido a la ONGEI y el correo electrónico.

Tabla 9. **Relación de las Instituciones que respondieron a la encuesta.**

Nombre de la Institución	Completo encuesta?	Medio
1. Despacho Presidencial (DP)	SI	Oficio y Correo Electrónico
2. Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA)	SI	Oficio y Correo Electrónico
3. Dirección Nacional de Inteligencia (DINI)	SI	Oficio y Correo Electrónico
4. Instituto Nacional de Defensa Civil (INDECI)	SI	Oficio y Correo Electrónico
5. Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI)	SI	Oficio y Correo Electrónico
6. Instituto Nacional de Estadística e Informática de Perú (INEI)	SI	Oficio y Correo Electrónico
7. Instituto Nacional de Radio y Televisión Peruana (IRTP)	SI	Oficio y Correo Electrónico
8. Cuerpo General de Bomberos Voluntarios del Perú (CGBVP)	SI	Oficio y Correo Electrónico
9. Sierra Exportadora (SE)	SI	Oficio y Correo Electrónico
10. Centro Nacional de Planeamiento Estratégico (CEPLAN)	SI	Oficio y Correo Electrónico
11. Autoridad Nacional del Servicio Civil (SERVIR)	SI	Oficio y Correo Electrónico
12. Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre (OSINFOR)	SI	Oficio y Correo Electrónico
13. Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN)	SI	Oficio y Correo Electrónico
14. Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL)	SI	Oficio y Correo

		Electrónico
15. Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (OSITRAN)	SI	Oficio y Correo Electrónico
16. Superintendencia Nacional de Servicios de Saneamiento (SUNASS)	SI	Oficio y Correo Electrónico

3.13 Validez y Confiabilidad

A fin de velar por la validez y la confiabilidad de la información cuantitativa se realizó la consistencia de datos para velar por la calidad de los mismos a fin de que se minimice la cantidad de errores y omisiones que se presentan generalmente dentro de la recolección de la información.

Se valora la fiabilidad de los informantes y se da por supuesto la idoneidad, conocimientos, credibilidad, imparcialidad, disposición para responder al cuestionario dado su jerarquía y responsabilidad.

Dentro de este contexto, se realizó correcciones a la pregunta II 6, por que durante la revisión se detectó error de interpretación al sentido de la pregunta de parte de los encuestados.

En la pregunta referida, se pide a los encuestados que establezcan un orden de más a menos los factores que según su opinión habían influido más en el no cumplimiento de la implementación de la norma en sus respectivas Instituciones, se coordinó telefónicamente con cada uno de ellos para una mejor explicación de lo que se perseguía, por lo que se les volvió a remitir por correo electrónico la pregunta, la cual; luego fue respondida por todos satisfactoriamente.

3.14 Resumen

A través de la investigación se ha logrado un análisis exhaustivo de la situación relacionado con la implementación de la NTP 17799 en las

Entidades del Sistema Nacional de Informática del Estado del Sector de Gobierno Nacional y adscritas a la Presidencia del Consejo de Ministros PCM y que tienen su Sede en la ciudad de Lima, que nos permite dar un aporte al conocimiento de la situación actual de la implementación de la Norma Técnica de Seguridad de la Información en estos organismos y explicar el por qué de la situación en que se encuentran en el proceso de implementación, así como dar las recomendaciones para superar las principales causas o factores que dificultan la implantación de la Norma Técnica NTP-ISO/IEC 17799.

Este, conocimiento logrado producto del análisis, las conclusiones y recomendaciones podrá compartirse con otras entidades de la esfera pública para impulsar, fortalecer y difundir la implementación de la norma y por lo tanto apalancar la consolidación del proyecto de Gobierno Electrónico del Perú. El fin último es que la implementación de la NTP 17799 código de buenas prácticas de la seguridad de la información en el estado se pueda acelerar tomando acción sobre las causas principales que se determinan dentro del presente estudio, y por lo tanto el uso y la gestión de la misma sea eficaz y eficiente, y esté alineado adecuadamente a la estrategias de la agenda digital Peruana en el marco de la sociedad de la información. Y consecuentemente fortalecer la confianza de la ciudadanía en el uso de los medios electrónicos para su interacción con el estado de esta forma impulsar el desarrollo de Gobierno electrónico en el Perú y la modernización del país.

En el siguiente capítulo presentaremos y analizaremos la información recolectada a través de la encuesta.

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE DATOS

El estudio comprende la presentación y el análisis de los datos recopilados mediante el software estadístico. SPSS 15.0.

Según el modelo de investigación y las hipótesis planteados, se presenta y se analiza la información recopilada a través de la encuesta primero: Sobre el nivel de valoración que las instituciones objeto de la investigación le atribuyen a la norma, segundo sobre el proceso de implementación desarrollado, tercero sobre los factores críticos y su influencia en el cumplimiento de la implementación y por último el nivel de madurez o progreso alcanzado a la fecha de realización del estudio, el detalle de los resultado se puede apreciar en el Anexo No 4 del estudio.

4.1 Presentación y Análisis de los Datos

4.1.1 El Nivel de valoración de la Norma por parte de la Institución

Corresponde a la primera parte de la encuesta, que contiene una plantilla de valoración en una escala de 1 a 6, considerando para cada uno de las 11 dimensiones o dominios de la norma.

H1: No hay la convicción suficiente de que la norma NTP de Seguridad de la Información agregue valor para la Institución por parte de los responsables de la implementación

En general la norma es valorada por la mayoría de las entidades objeto del estudio: 6 (38%) de ellas consideran que provee valor, otros 6 (38%) estiman que provee valor adicional y para 02 (13%) de ellos considera que es crítico para el éxito de la Institución. Aunque 02(13%) de las instituciones caen dentro de aquellos que consideraron que agrega poco o nada de valor, hacemos notar que SUNASS y OSITRAN son las que menos valoran la Norma.

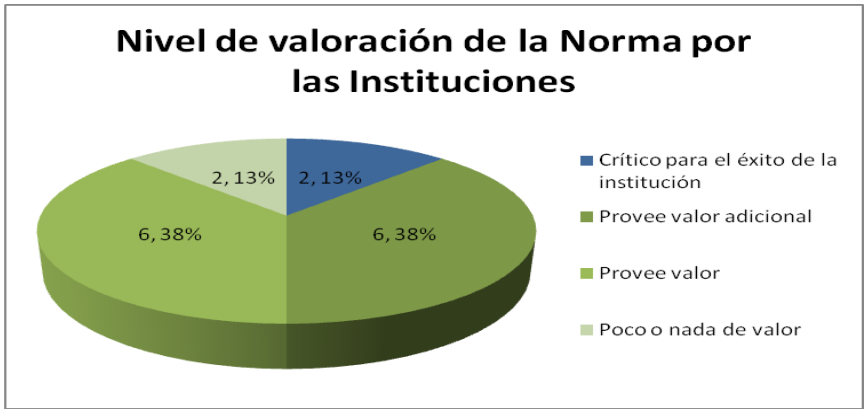

Grafico 10. **Gráfico del nivel de valoración de la Norma por Instituciones**

El gráfico No. 9 representa el número de intituciones y el porcentaje correspondiente del resultado de la encuesta el cual fue comentado anteriormente.Como se puede apreciar en la tabla No. 9 Indecopi y DINI son las Instituciones que le dan el mayor nivel de valoración a la norma.

Tabla 10 **Tabla de valoración de la Norma por Instituciones y por Dominios**

	DOMINIOS DE LA NORMA NTP ISO/IEC 17799:2007												
INSTITUCIÓN	Política de Seguridad de la Información	Organización de la Seguridad de la Información	Gestión de Activos	Seguridad de R. Humanos	Seguridad física y ambiental	Gestión de las Comunicaciones y Operaciones	Control de acceso	Adquisición, Desarrollo y Manto. de Sistemas de Información	Gest. Incidencias	Gestión de la Continuidad del negocio	Cumplimiento	Promedio General	Valoración por la Institución
INDECOPI	4,3	4,3	4,3	5,0	5,0	5,0	5,0	4,0	5,0	5,0	4,5	4,7	Crítico para el éxito de la institución
DINI	4,3	5,0	5,0	5,0	3,0	5,0	5,0	5,0	5,0	5,0	4,0	4,7	Crítico para el éxito de la institución
OSINERGMIN	4,0	3,7	4,7	4,0	5,0	4,5	4,0	4,0	5,0	5,0	4,5	4,4	Provee valor adicional
INDECI	4,0	4,0	4,0	4,0	4,0	5,0	4,0	5,0	4,0	5,0	4,0	4,3	Provee valor adicional
SERVIR	4,0	4,0	3,7	4,5	5,0	4,5	5,0	4,5	4,0	4,0	3,0	4,2	Provee valor adicional
SE	3,3	2,7	3,0	3,0	4,0	4,0	3,0	5,0	3,0	5,0	5,0	3,7	Provee valor adicional
INEI	3,0	4,0	3,7	3,0	4,0	4,5	4,0	3,5	3,0	4,0	4,0	3,7	Provee valor adicional
DP	3,0	3,0	3,7	4,0	4,0	4,0	4,0	3,5	4,0	4,0	3,5	3,7	Provee valor adicional
OSINFOR	3,0	3,0	4,0	4,0	4,0	4,0	4,0	3,5	3,0	3,0	3,0	3,5	Provee valor
OSIPTEL	3,0	3,3	4,0	4,0	3,0	3,5	4,0	3,5	3,0	4,0	3,0	3,5	Provee valor
CEPLAN	3,0	3,0	3,0	3,0	4,0	3,0	4,0	3,0	3,0	3,0	4,0	3,3	Provee valor
DEVIDA	3,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	Provee valor
I.R.T.P.	3,3	5,0	3,0	2,0	1,0	2,0	2,0	2,5	3,0	4,0	3,0	2,8	Provee valor
CGBVP	1,7	1,7	3,0	2,5	2,0	3,0	3,0	2,5	3,0	3,0	3,0	2,6	Provee valor
OSITRAN	1,0	1,0	1,0	1,0	1,0	3,0	2,0	1,0	1,0	1,0	1,0	1,3	Poco o nada de valor
SUNASS	4,0	4,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,7	Poco o nada de valor

Los dominios de mayor valoración promedio son: gestión de las comunicaciones y operaciones, control de acceso y Gestión de la continuidad del Negocio. Los 02 primeros corresponden a la parte tecnológica y el último a la parte organizativa de la norma.

El promedio global alcanzado para la valoración de norma es de 3.6 en una escala de 1 a 5 como se puede apreciar en la Tabla No 10. La calificación indica que la norma de seguridad provee valor adicional a las instituciones encuestadas.

Tabla 11. **Promedio Global de valoración de la Norma por dominios**

Dominio	Promedio de Valoración por Dominio	Valoración
Política de Seguridad	3,3	Provee valor
Organización de la seguridad de la información	3,4	Provee valor
Gestión de Activos	3,5	Provee valor
Seguridad de Recursos Humanos	3,5	Provee valor
Seguridad física y ambiental	3,5	Provee valor
Gestión de las Comunicaciones y Operaciones	3,9	Provee valor adicional
Control de acceso	3,7	Provee valor adicional
Adquisición desarrollo y Mantenimiento de Sistemas de Información	3,6	Provee valor adicional
Gestión de incidencias de Seguridad de la Información	3,5	Provee valor
Gestión de la Continuidad del Negocio	3,9	Provee valor adicional
Cumplimiento	3,5	Provee valor
Promedio Global	**3,6**	**Provee valor adicional**

Del resultado obtenido de la encuesta, el nivel de valoración global no confirma la hipótesis H1. Lo cual es un indicativo de que los encargados de la implementación de la norma de nuestra unidad de análisis, sí valoran positivamente y son conscientes de la importancia de la seguridad de la información para sus Entidades.

4.1.2 Proceso de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma

Esta sección corresponde a la segunda parte de la encuesta, donde se evalúa según las hipótesis correspondientes el proceso de implementación en las siguientes dimensiones: a) Inicio del proceso de implementación de la norma, b) adopción de una metodología para la

gestión del riesgo, c) definición del alcance del SGSI d) grado de dificultad en la aplicación de la norma según las cuatro etapas definidas por la ONGEI.

En esta parte, también los encuestados identifican de mayor a menor los factores que dificultan el cumplimiento de los plazos dados por el gobierno para el proceso de implementación.

H2: La Mayoría de las instituciones adscritas a la PCM no han iniciado el proceso de Implementación de la Norma de Seguridad de la Información, lo cual contribuye al atraso en la implementación en la administración pública.

El 56 % (9) de los encuestados manifiestan que su institución no ha iniciado el proceso de implementación de la NTP- ISO / IEC 17799.
De las personas (7) que respondieron que su institución había iniciado el proceso de implementación de la NTP –ISO / IEC 17799, el 100 % indicó que aún continúan en esa etapa.

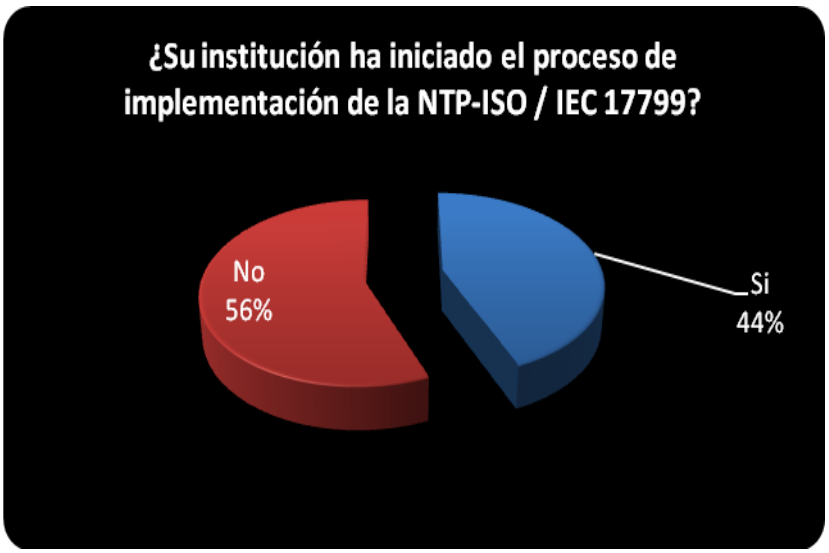

Grafico 11. **Gráfico del porcentaje de Instituciones que han iniciado la implementación de la Norma**

Tabla 12. **Porcentaje de instituciones que no han iniciado la implementación de la Norma**

Ítem	n	%
Si	7	43,8
No	9	56,3
Total	16	100,0

Los resultados confirman la hipótesis H2.

H2.1: El compromiso de la alta dirección, influye positivamente en el proceso de inicio y sostenimiento de la implementación de la NTP 17799, en los Organismos Descentralizados Adscritos a la PCM.

El apoyo visible y el compromiso de la alta gerencia es de muy alta influencia según el 62.5 %, el 31.3 % considera de alta influencia, apenas el 6.3 % considera de mediana influencia por lo que la Hipótesis H2.1 se confirma.

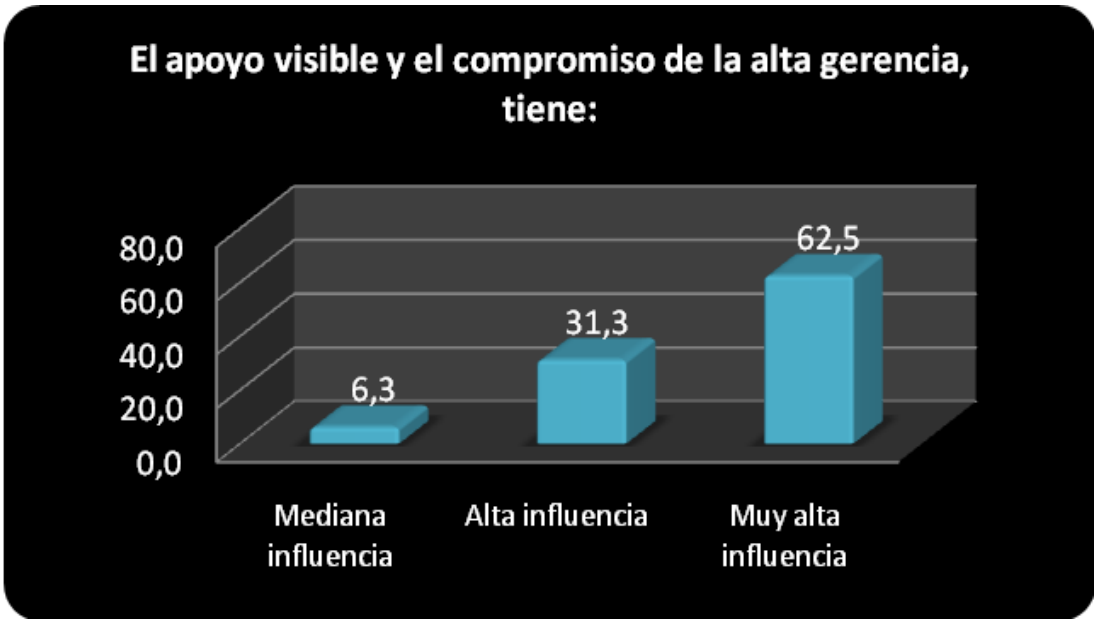

Grafico 12. **Gráfico del nivel del apoyo de la alta Gerencia respecto a la implementación de la Norma**

H2.2: La elección de una metodología para la gestión y evaluación de riesgos de los activos críticos facilita el encaminamiento del desarrollo del proceso de implementación de la norma.

La metodología que ha sido mayormente adoptada para la gestión y evaluación de riesgos es BS 7799 Parte 3 (60.0 %). Lo cual es indicador confirmativo de la hipótesis H2.2, lo que ha permitido que el 18% haya iniciado el proceso de evaluación.

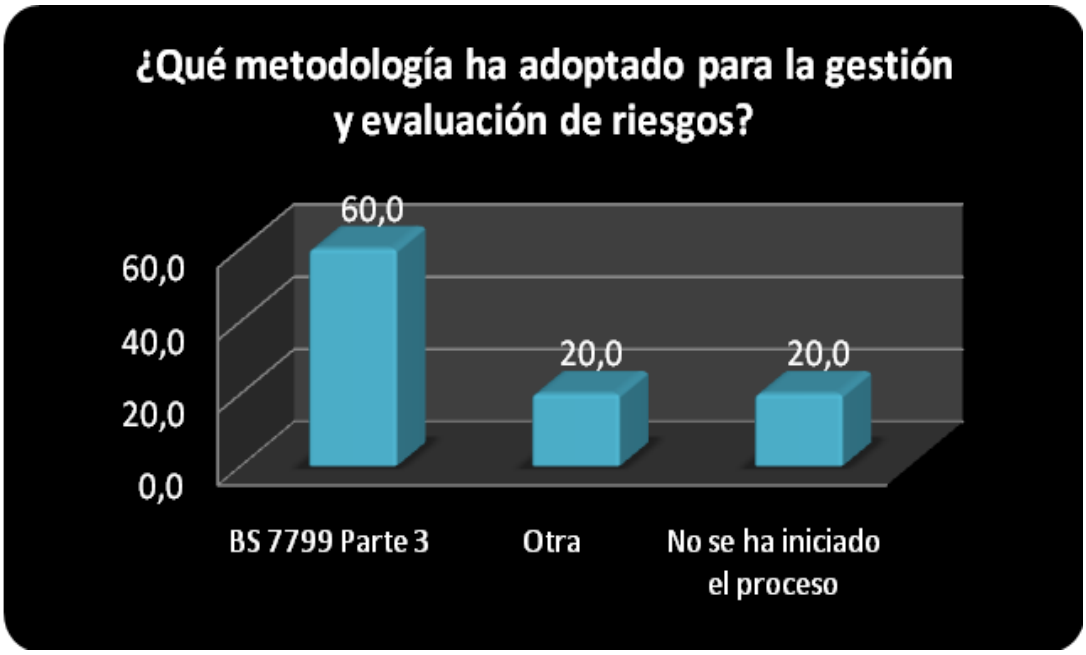

Grafico 13. **Gráfico de adopción metodología de gestión de Riesgos**

H2.3: Existe alto grado de dificultad en las etapas de implementación que contempla el modelo simplificado definido por la ONGEI, lo cual dificulta el avance en la implementación de la norma NTP 17799. Esta hipótesis se relaciona con el resultado dado en la tabla No 12 en la cual se registra que de las 16 Instituciones objeto del estudio sólo 6 (43.8 %) de 16 (56.3%) iniciaron el proceso de implementación.

4.1.3 Etapa I

I.1. Análisis e interpretación de los requerimientos de seguridad en base a la misión, visión y objetivos de la organización.

Los encuestados manifestaron que tuvieron: Nada de dificultad (17 %), Algo de dificultad (33 %), Mediana dificultad (17 %) y Alta dificultad (33 %) en esta etapa.

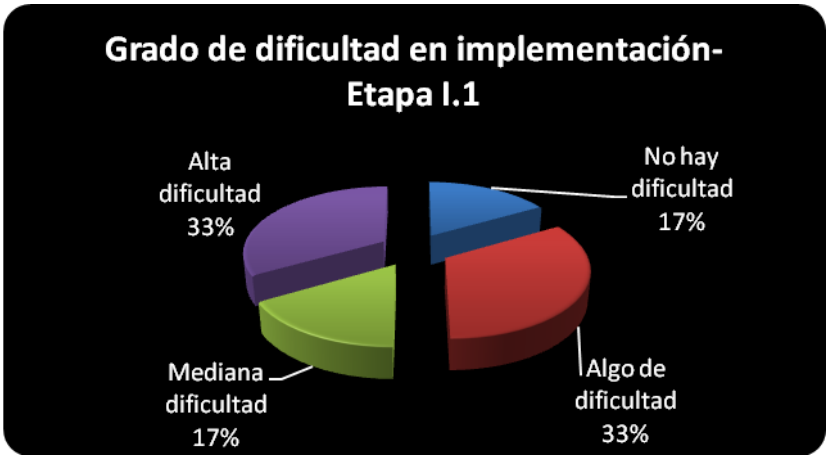

Grafico 14. **Gráfico del grado de dificultad análisis e interpretación de los requerimientos de seguridad.**

I.2. Identificación de los recursos (activos) dentro de los procesos de la organización

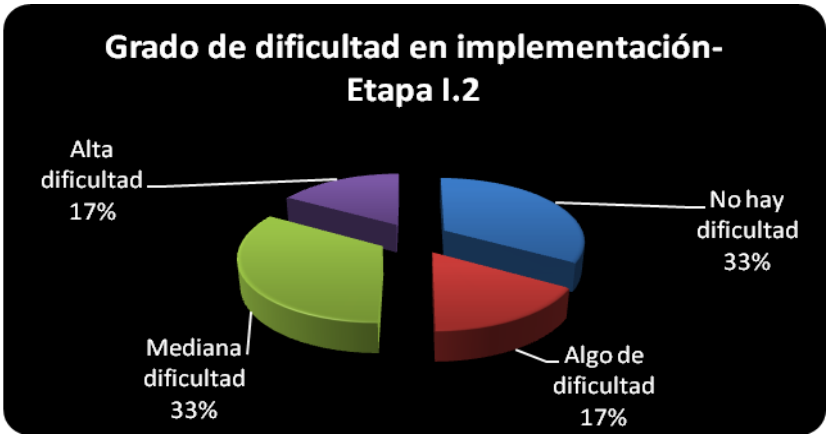

Grafico 15. **Gráfico del grado de dificultad identificación de Activos**

En la Etapa I.2 presenta 33% de aquellas instituciones que no presentaron ninguna dificultad, 17% algo de dificultad, 33% mediana y 17% alta dificultad.

4.1.4 Etapa II

II.1. Establecimiento de la Política de Seguridad de la organización

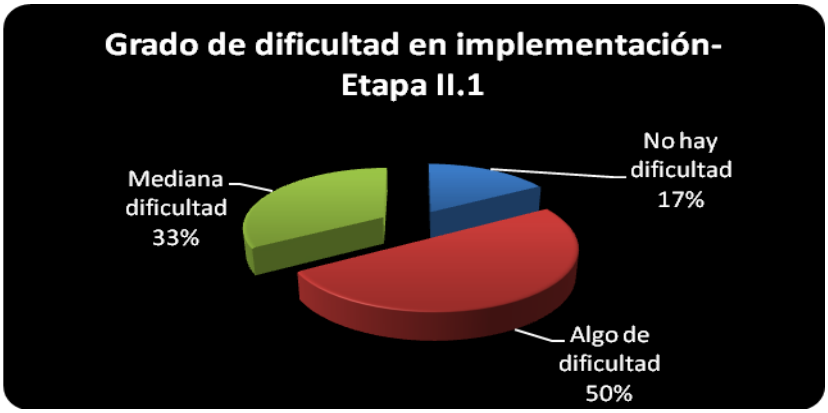

Grafico 16. **Gráfico del grado de dificultad establecimiento de la Política de seguridad**

El 17% manifiesta que no hay dificultad, El 50 % de las instituciones indican que tuvieron algo de dificultad y el 33% dificultad mediana en la implementación de la Etapa II.1.

II.2. Efectuar un análisis de riesgos

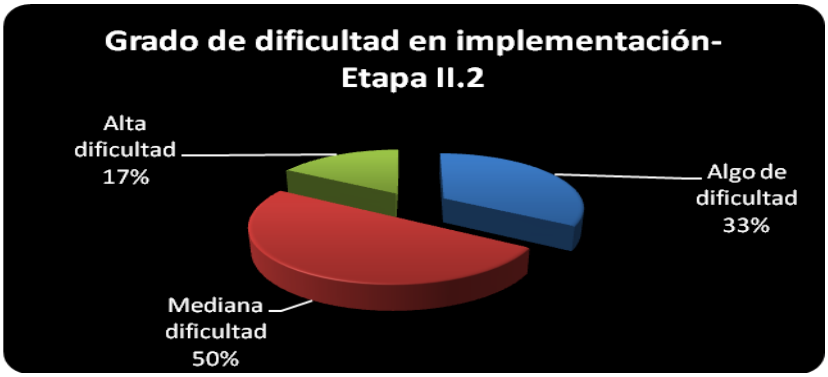

Grafico 17. **Gráfico del grado de dificultad análisis de Riesgos de seguridad**

Así mismo se observa en el gráfico que para el 33% representó algo de dificultad, para el 50 % de las instituciones presentaron mediana dificultad y para el 17% alta dificultad la implementación de la etapa II.2.

II.3. En base a los controles establecidos para cada dominio de la Norma, establecer la Brecha (Lo que se tiene y lo que falta implementar) SOA

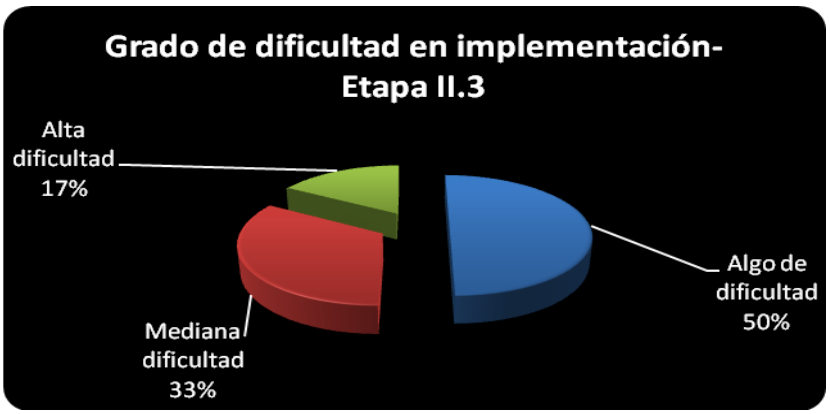

Grafico 18. **Gráfico del grado de dificultad establecimiento de la Brecha de Seguridad.**

El 50 % de las instituciones detallan que presentaron algo de dificultad en la implementación de la Etapa II.3, 33% mediana y 17% alta dificultad.

4.1.5 Etapa III

III.1. Establecimiento del documento del plan a 1,2 o 3 años

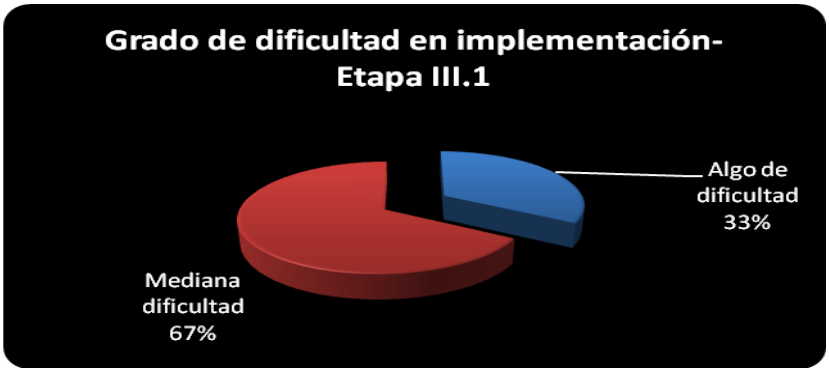

Grafico 19. **Gráfico del grado de dificultad establecimiento del plan de 1-3 años**

Un 67 % presentó mediana dificultad en la implementación de la Etapa III.1. y 33% algo de dificultad.

III.2. Implementación del Plan de Seguridad dentro del Plan Operativo Institucional (POI)

Grafico 20. **Gráfico del grado de dificultad para incorporar el Plan de seguridad en el POI**

Un 66 % de las instituciones presentaron entre algo y mediana dificultad en la implementación de la Etapa III.2., y para el 17% representó alta dificultad.

Destacamos dos aspectos que resultan clave dentro de las Instituciones objeto de la investigación y que está relacionada con la planificación. El 66%, de las Instituciones estudiadas manifiestan dificultades para el establecimiento del documento plan de actividades de 1,2 ó 3 años y su respectiva incorporación dentro del Plan Operativo Institucional (POI), sólo 2 de 7 que han iniciado el proceso de implementación han logrado reflejar presupuesto de sus actividades en su respectivo POI.

Así mismo, de la revisión de los documentos del Plan Estratégico respectivos y/o objetivos publicados en el portal de transparencia de cada Institución, se evidencia que no existe ninguna mención respecto a la

implementación de la Norma como objetivo estratégico ni actividad relacionada.

En tal sentido se confirma, que la Seguridad de la información no está comprendido dentro del proceso de planificación estratégica que realizan dichas Instituciones y por lo tanto no constituye un objetivo estratégico dentro de las instituciones estudiadas, no hay una plan establecido a nivel estratégico para la seguridad de la Información.

En consecuencia no hay metas y objetivos concretos a este nivel que se puedan reflejar con consistencia en el Plan Operativo y Presupuesto Institucional, como además manda la Ley 28411 Ley General del Sistema Nacional de Presupuesto, el cual señala claramente que el presupuesto Institucional se debe articular con el Plan Estratégico Institucional y que éste a su vez con el Plan Operativo Institucional (POI), de cada Institución.

4.1.6 Etapa IV

Consolidación de la estructura documental del sistema de Seguridad a Implementar.

IV.1. Entrega de la Política de Seguridad

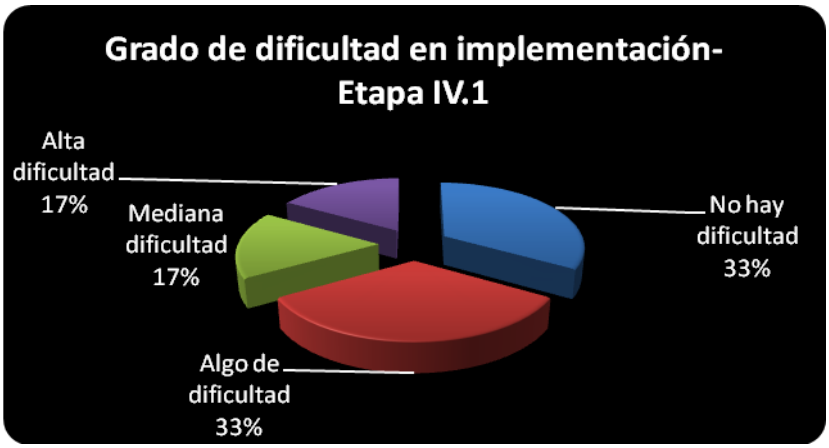

Grafico 21. **Gráfico del grado de dificultad entrega de la Política de seguridad.**

La implementación de la Etapa IV.1 representó para el 33% ninguna dificultad, 33% algo de dificultad, 17% mediana y el 17% alta dificultad.

IV.2. Entrega del Análisis de riesgos

Para el 50% representó algo de dificultad, 33% mediana y el 17% alta dificultad en la implementación de la Etapa IV.2.

IV.3. Entrega de la Brecha de lo implementado y lo que falta por Implementar

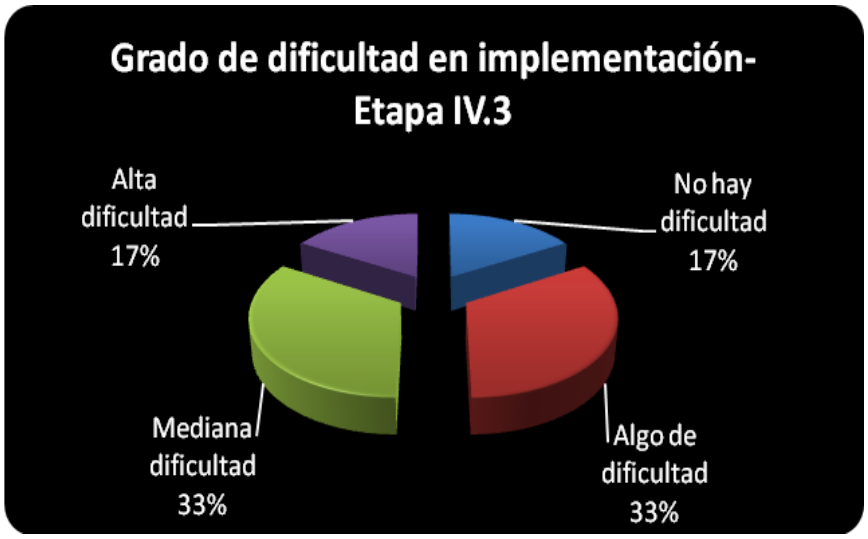

Grafico 22. **Gráfico del grado de dificultad para establecer el documento de declaración de aplicabilidad (Brecha)**

Una 33% de instituciones tuvieron algo, 33% mediana y 17% alta dificultad al implementar la Etapa IV.3.

IV.4. Plan de Seguridad de la Información (reflejado en el POI)

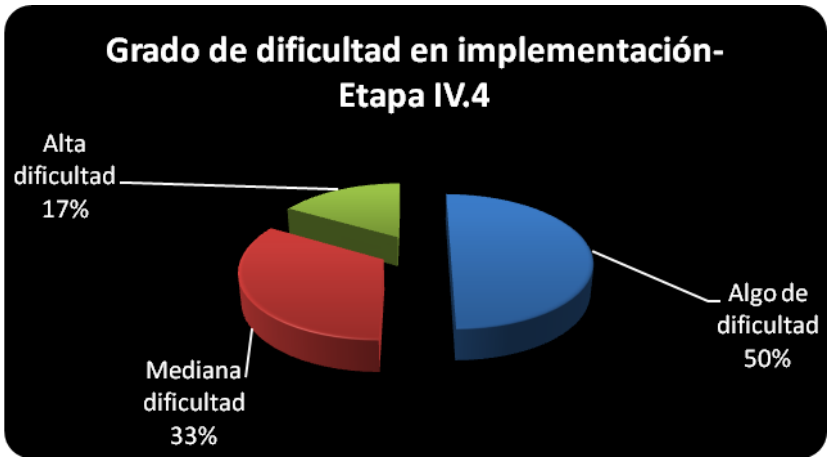

Grafico 23. **Gráfico del grado de dificultad para reflejar el plan de Seguridad en el Plan Operativo Institucional.**

Al igual que las demás etapas, la implementación de la Etapa IV.4 un 50 indicó que tuvo algo de dificultad, 33% mediana dificultad y el 17% alta dificultad.

H2.4: La falta de personal especializado y capacitación del personal dentro de las instituciones, influye negativamente en la implementación de la norma.

Los factores principales que dificultan el cumplimiento con los plazos de implementación de la Norma dadas por la PCM: Los entrevistados señalaron que en primer orden el factor que más dificulta es la falta de capacitación y concientización del personal, en segundo orden la falta de personal especializado en Seguridad de la Información, en el tercer orden el presupuesto insuficiente o no asignado, en cuarto orden la falta de un entendimiento cabal sobre la Seguridad de la información por parte de la alta dirección para apoyar con mayor efectividad estas iniciativas y así sucesivamente como se muestra en el cuadro de resultados. Es importante señalar en esta parte, que durante el proceso de implementación se ha

evidenciado también que hay dificultades para reflejar en el POI, las metas presupuestales para las actividades críticas que requiere la implementación de la Norma, del cual se deriva otros factores como los antes descritos y las que se presentan en la Tabla No. 13 y que constituyen barreras en el avance de implementación objeto de este estudio.

Se resalta el hecho de que en este orden CEPLAN consideró su reciente creación entre otros factores que han dificultado la implementación de la norma.

Tabla 13 **Orden de Factores que causan mayor dificultad en la implementación de la norma**

Factores que más dificultan en la implementación	0rden de dificultad
Falta de capacitación y concienciación del personal	1
Falta de Personal especializado en Seguridad de la información	2
Presupuesto Insuficiente o no asignado	3
Falta un entendimiento cabal sobre la Seguridad de la información por parte de la alta dirección para apoyar con mayor efectividad estas iniciativas	4
No se ha formalizado la creación del Área de Seguridad de la información y el responsable dentro de la institución	5
Dificultad en la gestión del proyecto y obtener los resultados esperados	6
Dificultad para cambiar la cultura organizacional orientado a la seguridad de la información (Resistencia al cambio)	7
Dificultad para alinear la seguridad de la información con los objetivos estratégicos de la institución (No se percibe el beneficio de la seguridad de la información)	8
Otros: Especificar…….CEPLAN es un organismo de reciente creación (2009), el cual tiene un plazo de tres años para culminar su estructuración.	9

Estos resultados confirman la hipótesis H2.4

H2.5: Existen dificultades en la gestión del proyecto y obtener resultados esperados debido a la falta de una cultura organizacional orientado a la seguridad de la información.

Esta hipótesis se confirma luego que la dificultad en la gestión del proyecto y obtener los resultados obtenidos se coloca en el sexto lugar entre los factores más influyentes para el logro de la implementación de la norma como se puede ver en la tabla No.13.

4.1.7 Grado de Influencia de los factores críticos en la implementación de la Norma

H3: El grado de influencia de los factores críticos es percibido como alta por los responsables de la implementación de la Norma lo cual influye positivamente en la implementación de la norma. Para la hipótesis los encuestados valoraron el grado de influencia de cada uno de los 10 factores identificados en la norma como sigue:

a) Una política, objetivos y actividades que reflejen lo objetivos de negocio de la organización.

El 56.3 % opina que una política, objetivos y actividades que reflejen los objetivos de negocio de la organización son de muy alta influencia.

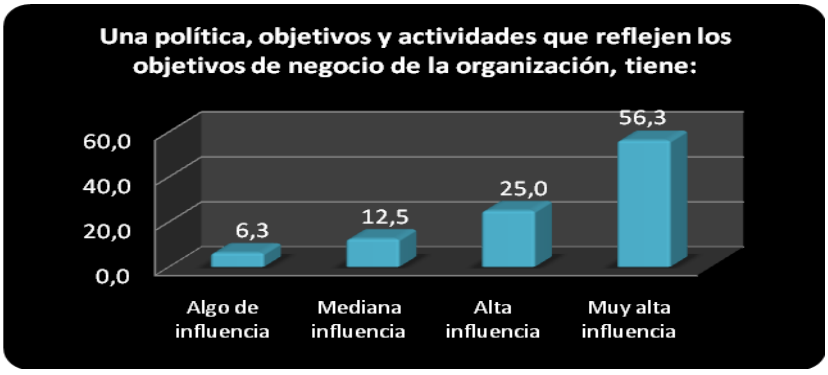

Grafico 24. **Gráfico del grado de Influencia del alineamiento de la Política con los Objetivos Institucionales.**

b) Un enfoque para implantar, mantener y monitorear e improvisar la seguridad que sea consistente con la cultura de la organización.

La mayor proporción de entrevistados (68.8 %) cree que un enfoque para implantar, mantener y monitorear e improvisar la seguridad que sea consistente con la cultura de la organización es de alta influencia.

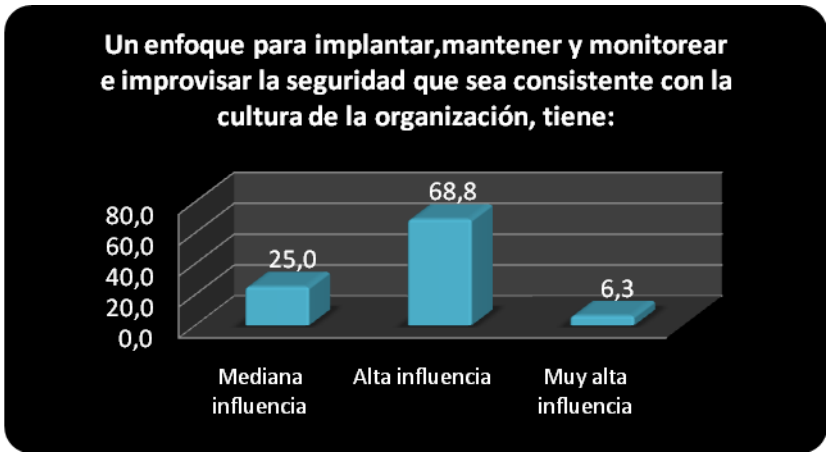

Grafico 25. **Gráfico del grado de Influencia del enfoque de la seguridad consistente con la cultura Institucional**

c) El apoyo visible y el compromiso de la alta gerencia.

El apoyo visible y el compromiso de la alta gerencia es de muy alta influencia según el 62.5 %.

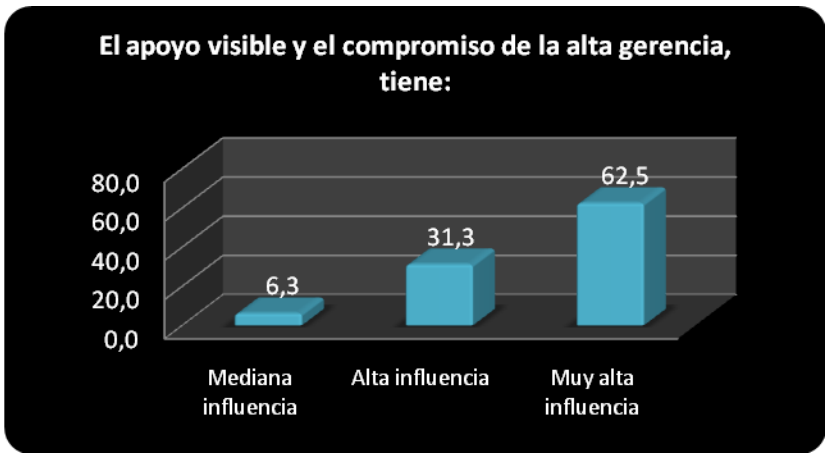

Grafico 26. **Gráfico del grado de Influencia del apoyo de la alta Dirección**

d) La buena compresión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo.

El 50 % de las instituciones bajo estudio creen que la buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo es de alta influencia.

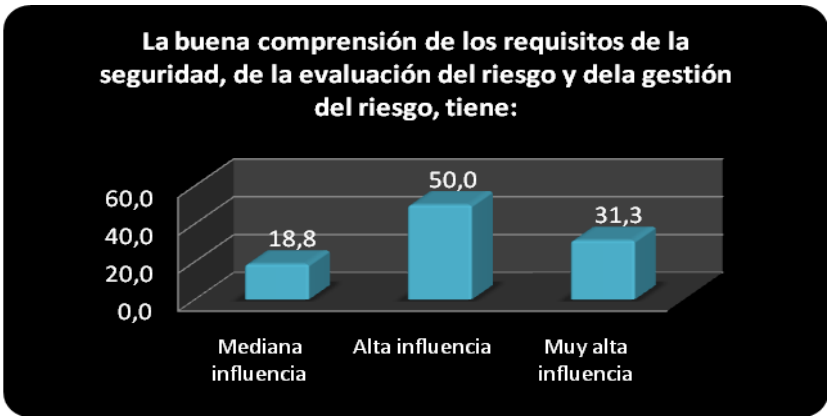

Grafico 27. **Gráfico del grado de Influencia de los requisitos y la gestión de riesgos.**

e) La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados.

Más del 90 % de los entrevistados indicaron que la convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados son de alta y muy alta influencia

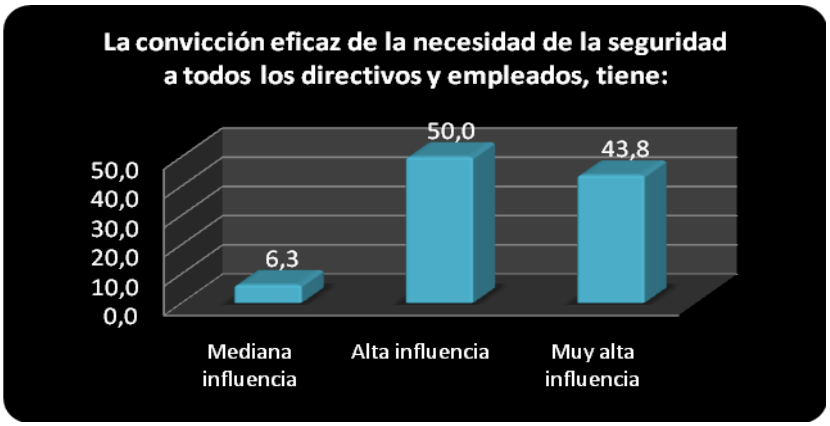

Grafico 28. **Gráfico del grado de Influencia de la convicción de los empleados y directivos de la necesidad de la seguridad de la información**

f) la distribución de guías sobre la política de seguridad de la información y de normas a todos los empleados y contratistas,

Las opiniones respecto a que influencia tendría la distribución de guías sobre la política de seguridad de la información y de normas a todos los empleados y contratistas son parcialmente parecidas, ya que un 37.5 % cree que es de mediana influencia y un cercano 31.3 % cree que es de alta influencia.

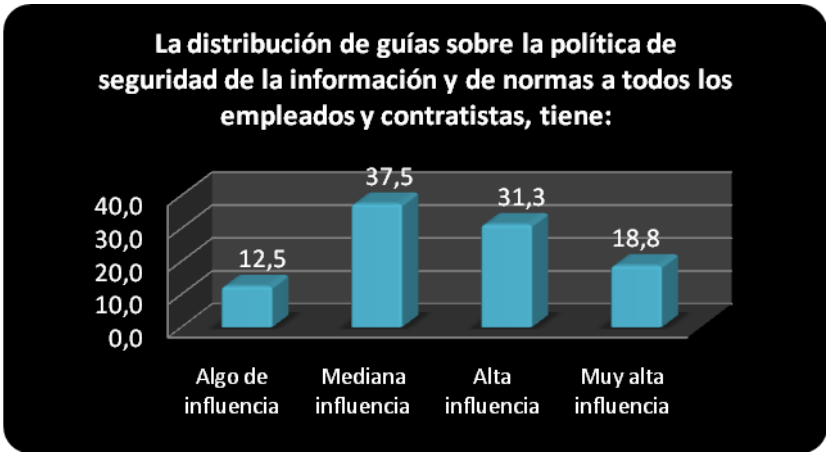

Grafico 29. ***Gráfico del grado de Influencia de la comunicación de la Política de seguridad a todos los empleados y contratistas.***

g) Aprovisionamiento para financiar actividades de gestión de la seguridad de la información.

El 68.8 % que representa la mayor proporción de entrevistados, indicaron que el aprovisionamiento para financiar actividades de gestión de la seguridad de la información es de alta influencia.

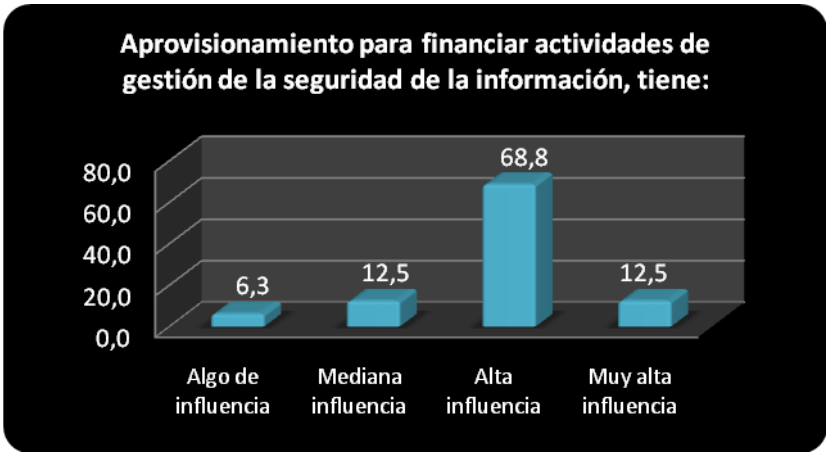

Grafico 30. **Gráfico del grado de Influencia del presupuesto para la gestión de la seguridad**.

h) la formación y capacitación adecuadas

Más del 50 % manifiesta que la formación y capacitación adecuada es de alta influencia, y un 37% considera de muy alta influencia.

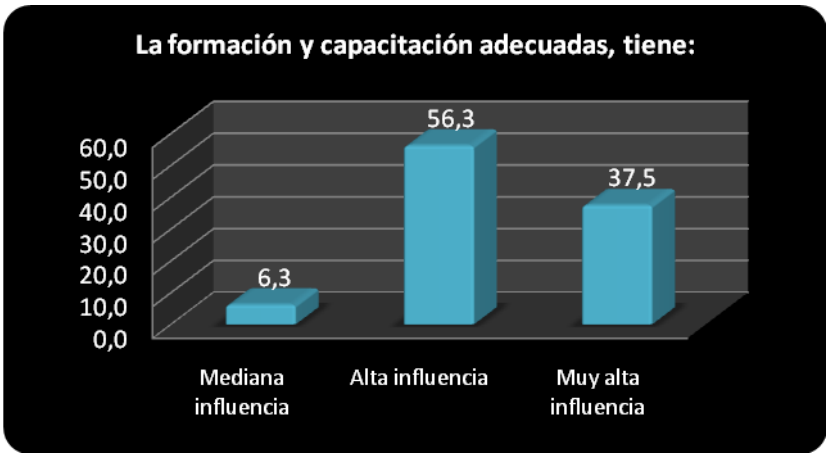

Grafico 31. **Gráfico del grado de Influencia de la formación y Capacitación**

i) Establecer un efectivo proceso de gestión de incidentes de la seguridad de la información.

Un 62.5 % cree que establecer un efectivo proceso de gestión de incidentes de la seguridad de la información es de alta influencia y un 18.8% considera de muy alta influencia.

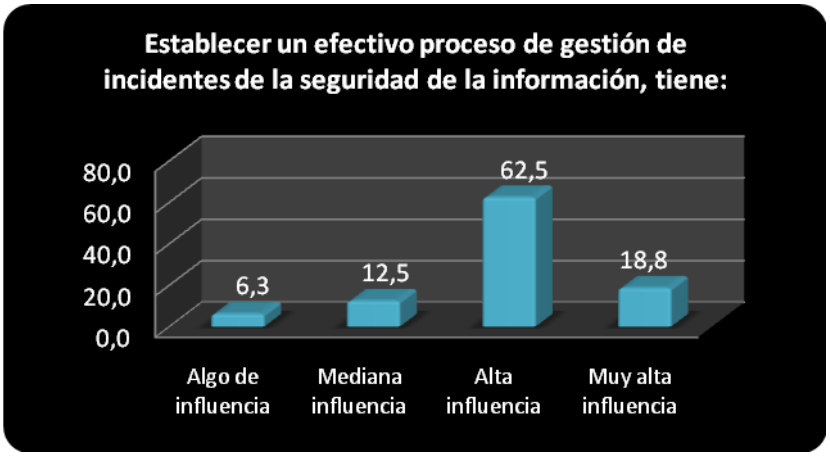

Grafico 32. **Gráfico del grado de Influencia de la gestión de incidentes de seguridad de la información.**

j) Un sistema integrado y equilibrado de medidas que permita evaluar el rendimiento de la seguridad de la información y sugerir medidas.

El 50 % cree que un sistema integrado y equilibrado de medidas que permita evaluar el rendimiento de la seguridad de la información y sugerir medidas es de alta influencia.

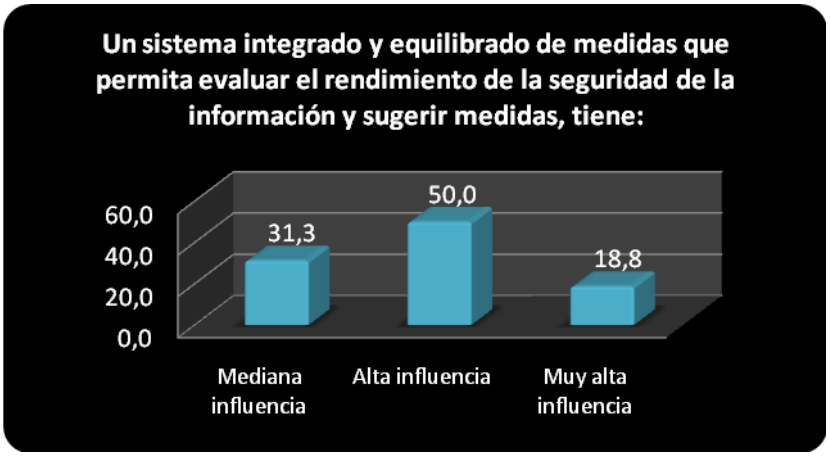

Grafico 33. ***Gráfico del grado de Influencia del establecimiento de medidas de rendimiento de la seguridad de la información***

H3.1: La formalización del Área de Seguridad, la cultura organizacional, el apoyo de la alta dirección y personal especializado tienen una alta influencia en la implementación exitosa de la Norma.

La formalización del área de Seguridad, el cambio en la cultura organizacional orientado a la seguridad, así como el apoyo de la alta gerencia se encuentran identificados entre los 08 más influyentes según lo obtenido en el ranking de la tabla No 13. En general hay un consenso sobre la influencia de los factores críticos para lograr el éxito en la implementación de la norma.

d) El Nivel de Madurez de la implementación de la norma por parte de la Institución

H.4 El nivel de madurez de la implementación de la norma se encuentra en la etapa inicial.

Mide, el nivel de los logros alcanzados por las Instituciones en la implementación de la Norma en una escala de 1 a 6.

Tabla 14. **Nivel de madurez de la implementación de la Norma por Instituciones**

	DOMINIOS DE LA NORMA NTP ISO/IEC 17799:2007												
INSTITUCIÓN	Política de seguridad	Organización de la seguridad de la información	Gestión de Activos	Seguridad de Recursos Humanos	Seguridad física y ambienta	Gestión de las comunicaciones y operaciones	Control de accesos	Adquisición, Des. y Manto. de Sistemas de Información	Gestión de Incidencias	Gestión de la Continuidad del negocio	Cumplimiento Legal	Promedio General	Nivel de madurez
INDECOPI	5,0	4,7	4,7	5,0	5,0	5,0	5,0	4,0	4,0	4,0	4,5	4,6	Gestionado
DINI	4,3	5,0	2,3	5,0	5,0	6,0	5,0	5,0	5,0	1,0	4,0	4,3	Gestionado
OSINERGMIN	3,3	3,0	4,7	4,5	5,0	4,0	5,0	5,0	3,0	5,0	3,5	4,2	Gestionado
DP	3,0	3,0	3,3	4,5	5,0	5,0	4,0	5,0	3,0	5,0	5,0	4,2	Gestionado
INDECI	5,0	5,0	4,0	4,0	4,0	4,5	4,0	5,0	3,0	2,0	3,0	4,0	Gestionado
OSIPTEL	3,3	3,0	3,0	4,0	4,0	3,5	4,0	3,0	2,0	5,0	3,0	3,4	Definido
SUNASS	4,7	4,3	3,0	3,0	3,0	3,5	3,0	3,5	3,0	3,0	3,0	3,4	Definido

Tabla 15. **Nivel de madurez de la implementación de la Norma por dominios**

Dominio de la Norma	Promedio de Nivel de madurez por Dominio	Nivel de madurez
Política de Seguridad	4.09	Gestionado
Organización de la seguridad de la información	3.86	Definido
Gestión de Activos	3.57	Definido
Seguridad de Recursos Humanos	4.29	Gestionado
Seguridad física y ambiental	4.43	Gestionado
Gestión de las Comunicaciones y Operaciones	4.50	Gestionado
Control de acceso	4.29	Gestionado
Adquisición desarrollo y Mantenimiento de Sistemas de Información	4.36	Gestionado
Gestión de incidencias de Seguridad de la Información	3.29	Definido
Gestión de la Continuidad del Negocio	3.57	Definido
Cumplimiento Legal	3.71	Definido
Promedio Global	**3.99**	**Definido**

El resultado de la encuesta arroja que del grupo que ha iniciado la implementación de la Norma alcanza un promedio global de nivel de madurez de 3.99, es decir en proceso de definición en una escala de 1 a 6.

Este resultado tiene dos aspectos primero, considerando las 7 Instituciones que han iniciado el proceso de implementación que llamaremos Grupo 1 (G1) que representa el 44%, segundo; Grupo 2 (G2) compuesta por 9 de las 16 instituciones que no han iniciado el proceso, representando el 56% que se ubica en el nivel de madurez no implementado (1), ponderando ambos niveles es decir 3.99 para el grupo que ha iniciado la implementación y 1 para los que no, este valor se reduce a 0.88.

Nivel de Madurez Ponderado de la muestra:

= (G1 (3.999)*0.44)+(G2(1)*0.56))/2=1.16, este nivel cae cercano al nivel 1 de calificación Inicial, por lo tanto la Hipótesis H4 se confirma.

Tabla 16. **Tabla Resumen de Validación de Hipótesis**

Variable	Hipótesis	Resultado
a) El Nivel de valoración de la Norma por parte de la Institución	H1: No hay la convicción suficiente de que la norma NTP agregue valor para la Institución	No Se confirma
b) Proceso de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma	H2: La Mayoría de las instituciones adscritas a la PCM no han iniciado el proceso de Implementación de la Norma, lo cual influye negativamente en el nivel de Madurez de la implementación.	Se confirma
	H2.1: El compromiso de la alta dirección, influye positivamente en el proceso para una implementación exitosa de la NTP, 17799, en los Organismos Descentralizados Adscritos a la PCM.	Se confirma
	H2.2: La elección de una metodología para la gestión y evaluación de riesgos de los activos críticos facilita el encaminamiento del desarrollo del proceso de implementación de la norma.	Se confirma
	H2.3: Existe alto grado de dificultad en las etapas de implementación que contempla el modelo simplificado definido por la ONGEI, lo cual dificulta el avance en la implementación de la norma NTP 17799	Se confirma
	H2.4: La falta de personal especializado y capacitación del personal dentro de las instituciones, influye negativamente en la implementación de la norma.	Se confirma
	H2.5: Existen dificultades en la gestión del proyecto y obtener resultados esperados debido a la falta de una cultura organizacional orientado a la seguridad de la información.	Se confirma

c). Grado de Influencia de los factores críticos en la implementación de la Norma	H3: El grado de influencia de los factores críticos es percibido como alta por los responsables de la implementación de la Norma lo cual influye positivamente en la implementación de la norma.	Se confirma
	H3.1: La formalización del Área de Seguridad, la cultura organizacional, el apoyo de la alta dirección y personal especializado tienen una alta influencia en la implementación exitosa de la Norma.	Se confirma
d) El Nivel de Madurez de la implementacion de la norma por parte de la Institución	H.4 El nivel de madurez de la implementación de la norma se encuentra en la etapa inicial	Se confirma

4.1.8 Preguntas de la encuesta sobre aspectos complementarios

Parte II pregunta 7.- Según su opinión la responsabilidad de la seguridad de la información en una organización es:

Un 50% de los encuestados conisderan que la responsabilidad de la seguridad de la información es una responsabilidad global de la Institución, un 25% de la alta dirección, 19% del Gerente de Sistemas, 6% del jefe de Seguridad. Estos resultados demuestran que el 50% de los que toman el liderazgo en la implementación de la norma aún no tieene claro que la responsabilidad de la seguridad de la Información es global.

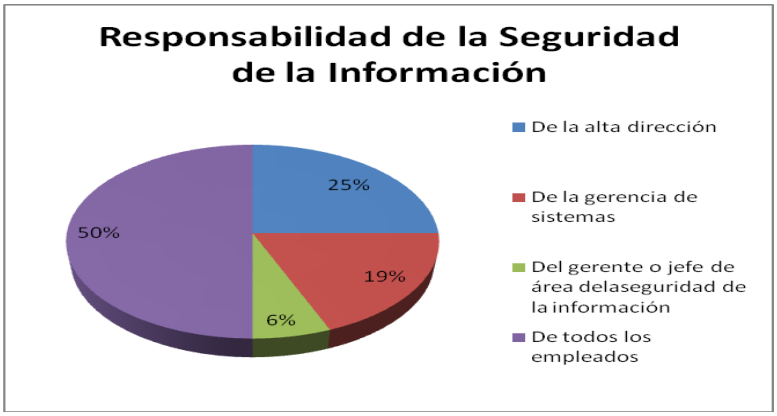

Grafico 34. **Gráfico sobre la respuesta de los encuestados respecto de quién es la responsabilidad de la seguridad de la información**

Parte II Pregunta 8: Según su opinión para efectivizar el cumplimiento de la implementación de la norma la ONGEI: (Puede marcar más de uno).

El 69% considera que la ONGEI debería realiazar una auditoría de cumplimient, el 31 % que debe apoyar con consultorías especializadas.Este resultado evidencia la necesidad de que la ONGEI en su condición de encargada por la PCM como ente rector del Sistema Nacional de Informática debería implementar un sistema de control y acompañamiento para impulsar la implementación de la Norma.

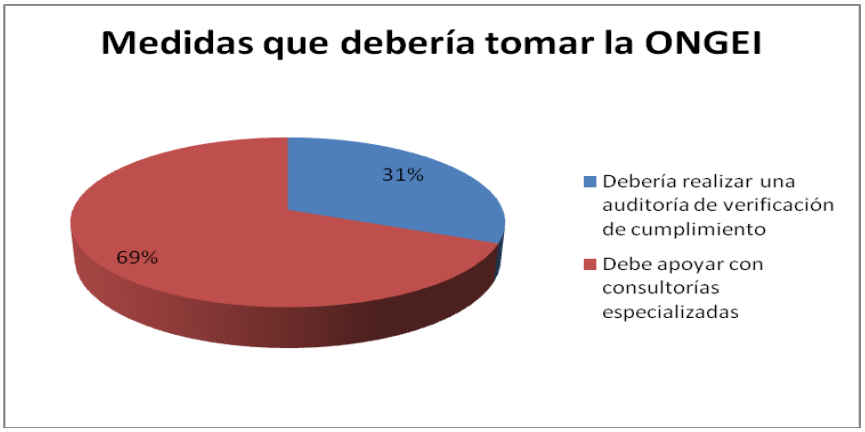

Grafico 35. **Gráfico sobre las medidas que debería tomar la ONGEI para impulsar la implementación de la Norma en las entidades del Estado.**

Parte III Pregunta 3: Según su apreciación, las herramientas (Seguridad de la información/Documentos/Plantillas) disponibles en el Portal de la ONGEI.

El 57% considera que las herramientas de seguridad de la información disponibles en el portal de la ONGEI son medianamente útiles, y un 43 % opina que son muy útiles.

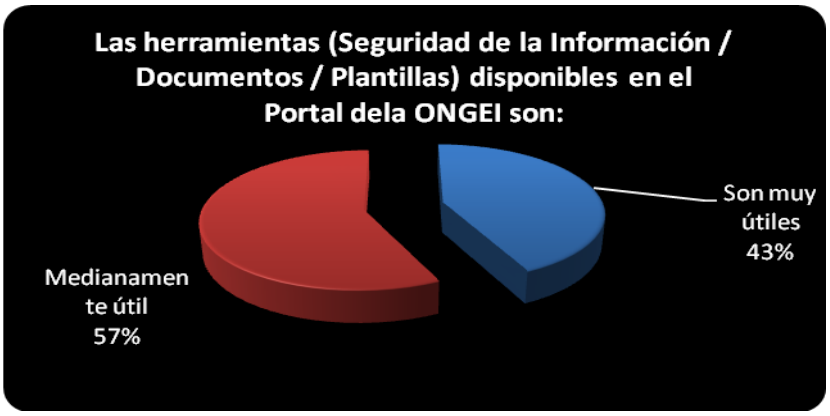

Grafico 36. **Gráfico del grado de utilidad para los encuestados de las guías, herramientas y plantillas disponibles en el portal de la ONGEI.**

4.2 Enlace entre los factores encontrados en las investigaciones previas y las del proyecto

Durante la etapa de revisión de la literatura, se puede destacar estudios realizados como el de “Critical success factors and requirements for achieving business benefits from information security” (Partida, Ezingerad, 2007), este estudio tiene un enfoque general sobre los factores críticos de éxito en la implementación de los Sistemas de Gestión de seguridad de la Información en general, no se orienta a ningún sector ni norma de seguridad en específico, sin embargo aportó a nuestro estudio pautas para el diseño de nuestro modelo de investigación.

En España la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), realizó un estudio con el objetivo de obtener los datos que permitieran conocer el grado de implantación de la seguridad de los sistemas de la información en las empresas entrevistadas de acuerdo con la Norma ISO/IEC17799:2000 , la encuesta se aplicó a 40 empresas de distintos sectores y complementariamente al objetivo del estudio en dichas empresas se identificaron algunos factores que dificultan su implementación.

Los resultados muestran que el grado de implantación de las recomendaciones de la norma son muy inferiores (53%) a lo que sería deseable (90%).

a) El mayor obstáculo a la implantación de la seguridad es la cultura empresarial, por encima de los problemas que a priori podrían parecer más relevantes como presupuesto o tecnología. b) Las organizaciones consideran que un porcentaje muy elevado de las recomendaciones de seguridad no les son aplicables. Únicamente entre un 5% y un 10% de las recomendaciones pueden no ser aplicables en función de la naturaleza de la organización, por lo que realmente las respuestas de controles no aplicables, realmente reflejan problemas de desconocimiento, más que de no aplicabilidad. c) El nivel de desconocimiento de los distintos aspectos que condicionan la seguridad es también más alto de lo que cabía esperar.

En el Perú, encontramos un estudio en el Sector Privado para determinar en qué medida la aplicación de las Normas ISO 27001 y 27002 sobre Seguridad de la Información beneficia a las pequeñas y medianas empresas de la región Lambayeque por Msc Ing. Jessie Leila Bravo Jaico (Valoración), su objetivo no se orienta a determinar las causa o los niveles de implementación de la norma.

Los estudios realizados antes mencionados como se puede apreciar de lo expuesto, tienen distintos objetivos y un enfoque general sobre la implementación del sistemas de seguridad de la información sin embargo

aporta elementos que han servido de base para la realización del presente estudio en la cual enfocamos específicamente la problemática de la implementación de la norma NTP ISO/IEC 17799 en el sector público del país.

En tal sentido es la primera vez que se acomete un estudio de esta naturaleza en Perú y en el sector con el propósito de averiguar los problemas fundamentales que enfrenta el Gobierno Nacional en el proceso de implementación de esta importante norma cuyas conclusiones y recomendaciones las cuales que se presentan en el siguiente y último capítulo, pretenden ser un aporte al plan integral de seguridad de la información en la administración pública comprendido en la Agenda Digital Peruana, orientado a la generación de confianza y seguridad en la ciudadanía y empresas e impulsar el logro de los objetivos estratégicos del proyecto de Gobierno Electrónico para una modernización más acelerada del país dentro de un contexto cada vez más globalizado y complejo.

CAPÍTULO V . CONCLUSIONES Y RECOMENDACIONES

La recolección de la información para la investigación fue realizada mediante una encuesta que fue formalizada por la ONGEI mediante un oficio múltiple a los 16 Organismos Públicos Adscritos a la Presidencia del Consejo de Ministros (PCM), los cuales están incluidos en el presente estudio. La muestra tiene carácter intencionado y no probabilístico debido a las razones expuestas en el punto correspondiente.

La encuesta fue respondida por el 100% de los responsables de las unidades de informática cuyo cargo tiene mayoritariamente la denominación de Jefes de Informática, Gerentes y Directores de la Entidad respectivamente.

Se planteó cuatro tipos de hipótesis, a saber: Sobre la valoración de la norma por las instituciones, el proceso de implementación y la influencia de los factores críticos en la implementación, el nivel de madurez o logros alcanzados en el proceso de la implementación. Son un total de 11 Hipótesis cuyos resultados se resumen en el siguiente cuadro:

Variable	Hipótesis	Resultado
a) El Nivel de valoración de la Norma por parte de la Institución	H1: No hay la convicción suficiente de que la norma NTP agregue valor para la Institución	No Se confirma
b) Proceso de Implementación del Sistema de Gestión de Seguridad de la Información	H2: La Mayoría de las instituciones adscritas a la PCM no han iniciado el proceso de Implementación de la Norma, lo cual influye negativamente en el nivel de Madurez de la implementación.	Se confirma

(SGSI) basado en la Norma	H2.1: El compromiso de la alta dirección, influye positivamente en el proceso para una implementación exitosa de la NTP, 17799, en los Organismos Descentralizados Adscritos a la PCM.	Se confirma
	H2.2: La elección de una metodología para la gestión y evaluación de riesgos de los activos críticos facilita el encaminamiento del desarrollo del proceso de implementación de la norma.	Se confirma
	H2.3: Existe alto grado de dificultad en las etapas de implementación que contempla el modelo simplificado definido por la ONGEI, lo cual dificulta el avance en la implementación de la norma NTP 17799	Se confirma
	H2.4: La falta de personal especializado y capacitación del personal dentro de las instituciones, influye negativamente en la implementación de la norma.	Se confirma
	H2.5: Existen dificultades en la gestión del proyecto y obtener resultados esperados debido a la falta de una cultura organizacional orientado a la seguridad de la información.	Se confirma
c). Grado de Influencia de los factores críticos en la implementación de la Norma	H3: El grado de influencia de los factores críticos es percibido como alta por los responsables de la implementación de la Norma lo cual influye positivamente en la implementación de la norma.	Se confirma
	H3.1: La formalización del Área de Seguridad, la cultura organizacional, el apoyo de la alta dirección y personal especializado tienen una alta influencia en la implementación exitosa de la Norma.	Se confirma
d) El Nivel de Madurez de la implementacion de la norma por parte de la Institución	H.4 El nivel de madurez de la implementación de la norma se encuentra en la etapa inicial	Se confirma

a) El Nivel de valoración de la Norma por parte de las Instituciones, los resultados muestran que los responsables de implementar la norma en las Instituciones valoran el aporte de la norma en un nivel de 3.6 en una escala de 5, nivel que según el resultado provee valor adicional a la Institución, contrario a lo que planteaba la hipótesis, pero esta valoración en la práctica no necesariamente se capitaliza a favor de la implementación, teniendo en cuenta que sólo el 44% de las instituciones encuestadas iniciaron la implementación.

b) Proceso de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma. El resultado obtenido para esta variable tiene varias dimensiones, el primero de ellos referido a identificar cuántos y qué instituciones habían iniciado el proceso de implementación, el resultado obtenido es que de de las 16 Instituciones de la muestra sólo 7 (44%) iniciaron y 9 (56%) no han iniciado el proceso.

   Para evaluar el proceso de implementación se tomó como referencia el modelo simplificado de implementación recomendado por la ONGEI. El resultado refleja que a pesar de que el modelo es simplificado es una herramienta valiosa, acometer cada etapa por parte de las instituciones es considerado de mediana a alta dificultad.
   Los aspectos a remarcar es que cuando se pregunta a los encuestados sobre el plan de implementación y su incorporación en el POI, la mayoría que es el 66% ha manifestado que les es difícil documentar y reflejar en el POI.

   Dentro de la encuesta, se solicita a los encuestados identificar y ordenar de mayor a menor los factores de dificultad en el proceso. El resultado mostró 8 factores la cuales se listan en la tabla No. 12, siendo los 4 primeros los siguientes:

   1. Falta de capacitación y concienciación del personal
   2. Falta de Personal especializado en Seguridad de la información
   3. Presupuesto Insuficiente o no asignado

4. Falta un entendimiento cabal sobre la Seguridad de la información por parte de la alta dirección para apoyar con mayor efectividad estas iniciativas.

   De los resultados anteriores, podemos deducir que los factores mencionados en orden de dificultad son derivativas del factor principal que está relacionado con el hecho de que la implementación de la norma no es incorporado dentro de los objetivos estratégicos de cada Institución, como resultado del planeamiento estratégico.

.

c) Grado de Influencia de los factores críticos en la implementación de la Norma. Los resultados en este aspecto demuestran que los encuestados consideran que los 10 factores identificados por la Norma tienen alta y muy alta influencia en el éxito en la implementación.

d) El Nivel de Madurez de la implementación de la norma logrado por parte de la Institución. El resultado de la encuesta sitúa la madurez de la implementación en el nivel inicial dentro de las Instituciones objeto del estudio, este nivel es fuertemente influenciado por el alto porcentaje (56.3%) de las instituciones que no han iniciado el proceso de implementación es decir sólo 7 de 16 instituciones estudiadas.

5.1 Conclusiones

1. Del resultado de la investigación se tiene que los organismos públicos descentralizados adscritos a la PCM, valoran la importancia de la Norma de Seguridad para la Institución, sin embargo esto no guarda relación con el nivel de implementación alcanzado.

2. Dentro del proceso de implementación Sólo 7 de las 16 Instituciones objeto del estudio han iniciado el proceso de implementación, se evidencia dificultad para establecer un plan documentado para 01 ó 3

años, así como la incorporación de dichos planes en los Planes Operativos Institucionales (POI).

3. En el mismo proceso de implementación, destacamos dos aspectos que resultan clave dentro de las Instituciones objeto de la investigación y que está relacionada con la aplicación de la metodología PDCA (planificación). El 66%, de las Instituciones estudiadas manifiestan dificultades para el establecimiento del documento plan de actividades de 1,2 ó 3 años y su respectiva incorporación dentro del Plan Operativo Institucional (POI), de la revisión de los documentos del Plan Estratégico respectivos y/o objetivos publicados en el portal de transparencia de cada Institución, se evidencia que no existe ninguna mención respecto a la implementación de la Norma como objetivo estratégico ni actividad relacionada.

   En tal sentido se confirma, de acuerdo al análisis que la Seguridad de la información no está comprendido dentro del proceso de planificación estratégica que realizan dichas Instituciones y por lo tanto no constituye un objetivo estratégico dentro de las instituciones estudiadas, no hay una plan establecido a nivel estratégico para la seguridad de la Información. En consecuencia no hay metas y objetivos concretos a este nivel que se puedan reflejar con consistencia en el Plan Operativo y Presupuesto Institucional, como además; manda la Ley 28411 Ley General del Sistema Nacional de Presupuesto, el cual señala claramente que el presupuesto Institucional se debe articular con el Plan Estratégico Institucional y que éste a su vez con el Plan Operativo Institucional (POI), de cada Institución.

4. No hay, un entendimiento claro sobre la responsabilidad global de la seguridad de la información dentro de la Institución, lo cual se refleja en que el nivel de liderazgo para la implementación mayormente descansa en los gerentes o jefes de Área de Informática y sin el

compromiso de la alta dirección, con un enfoque de seguridad informática más que a la Seguridad de la Información.

Por las razones expuestas, esta investigación, ha determinado que el bajo nivel alcanzado en la implementación de la Norma de Seguridad en los Organismos Públicos Descentralizados Adscritos a la PCM tiene como causa principal el hecho de que la Seguridad de la Información a pesar de formar parte de los objetivos estratégicos del plan de acción de la Agenda Digital Peruana, objetivo No. 5 desarrollo de Gobierno Electrónico, estrategia 5.1, acción No 6 “Desarrollo de un plan de seguridad de la información para el sector público”, y declarado obligatorio por resolución ministerial de la PCM desde el año 2004, no ha sido incorporado en el planeamiento estratégico de cada una de las Instituciones , no forma parte del conjunto de objetivos estratégicos del mismo y como consecuencia no se garantiza las metas presupuestarias correspondientes, dificultando la ejecución de los planes de corto, mediano y largo plazo del proyecto de implementación de la Norma.

5. Como consecuencia del punto anterior y del análisis de los resultados obtenidos en la investigación del proceso de implementación, ha sido posible identificar y calificar en orden de mayor a menor otros factores derivados que dificultan el proceso de implementación entre ellos en primer lugar, la capacitación y concienciación del capital humano, en segundo lugar la falta de Personal especializado en Seguridad de la información. Otro factor importante es la falta de formalización del Área de Seguridad de la Información dentro de las instituciones, pues al no existir una estructura organizativa oficial con roles definidos las actividades de implementación de la norma pierden prioridad dentro de la Institución.

6. Por otro lado, los encuestados también perciben, que en el proceso de Implementación de la norma en las Instituciones no hay un acompañamiento sistematizado del Organismo Rector (ONGEI) a

través de talleres o consultorías especializadas sobre la norma, tampoco un mecanismo de control para supervisar el desarrollo del mismo y sistematizar las lecciones aprendidas enmarcado en un plan maestro de Seguridad de la Información de las entidades públicas.

7. Los logros obtenidos en el proceso de implementación reflejan una madurez de nivel inicial dentro del grupo de Instituciones investigadas, la cual tiene relación con los principales factores que inhiben el proceso y que se señalan en los puntos anteriores.

5.2 Recomendaciones

En base a las conclusiones del presente estudio, se recomienda las siguientes líneas de acción destinadas a impulsar la implementación de la norma:

1. Se recomienda que la ONGEI en el marco de sus atribuciones disponga en forma obligatoria la incorporación de la seguridad de la información dentro del proceso de Planeamiento Estratégico de cada una de las Instituciones asegurando que las metas presupuestarias se reflejen en el POI de las Instituciones, en cumplimiento de la Ley 28411 Ley General del Sistema Nacional de Presupuesto.

2. Que la ONGEI, en su calidad de ente rector de la Entidades del Sistema Nacional de Informática del Estado; con INDECOPI como Autoridad Administrativa Competente y emisor de la Norma Técnica, y el SG1 organismo que genera estándares para el intercambio electrónico de datos firmen un convenio marco para conformar un grupo técnico de apoyo que establecerán un plan maestro de talleres de sensibilización orientado todos los titulares de las Instituciones públicas cuyo fin será proporcionarles un entendimiento claro sobre la necesidad de incorporar el gobierno de la Seguridad de la Información dentro del proceso de

Planeamiento Estratégico de sus respectivas entidades y el alineamiento con los objetivos estratégicos de la Agenda Digital Peruana y el proyecto de Gobierno Electrónico. Así mismo el Grupo Técnico de Apoyo, brindará asesoría especializada en la elaboración de metodologías y su aplicación a las instituciones durante el proceso de implementación de la Norma.

3. La PCM-ONGEI debe generar los lineamientos necesarios para aquellas Instituciones del Sistema Nacional de Informática requieran reformular sus respectivos Planes Estratégicos para cumplir con las recomendaciones del punto 1, y que todas las Instituciones procedan a la asignación formal de funciones y responsabilidades de la unidad o área de Seguridad de la Información con personal de su planta, designando un responsable con roles específicos sobre la Seguridad de la Información, quien deberá desarrollar el proyecto de implementación de la Norma y gestionar la incorporación del plan de actividades en el Plan Operativo Institucional (POI), correspondiente.

4. La PCM-ONGEI posibilite la creación de un organismo Auditor especializado independiente de Seguridad de la Información cuya función específica será desarrollar un programa de auditorías para auditar el proceso de implementación de la Norma de Seguridad de la Información en Entidades del Sistema Nacional de Informática del Estado. Así mismo dicho organismo realizará la capacitación de auditores de seguridad de la Información para el personal de la administración pública y determinará periódicamente el nivel de madurez alcanzado por cada Institución que será publicado en el portal de la PCM.

5. Que la ONGEI establezca un programa de becas de especialización en Seguridad de la Información u otro tipo de incentivos para el personal clave de las Instituciones por sectores,

que hayan obtenido la certificación ISO 27001 o que hayan demostrado logros sobresalientes en el proceso de implementación de la Norma, de acuerdo al Ranking determinado por los auditores oficiales y que será publicado en el Portal de la PCM.

5.3 Línea de tiempo de las recomendaciones

Las líneas de acción recomendadas se agrupan en dos niveles: a) Acciones a nivel de los Entes Rectores ONGEI-PCM (Color Rojo en la figura) b) Acciones a nivel de las Instituciones (Color Naranja).

La línea de tiempo de ejecución de las recomendaciones se realizará dentro del marco del Plan Estratégico Sectorial 20011-2016, para ello se hará entrega formal del Estudio a la ONGEI-PCM, luego de la sustentación. El Ente Rector podrá emitir las directivas y lineamientos según la recomendación número 1, se estima que el convenio ONGEI_ INDECOPI_SG1 y el programa de talleres de la sensibilización (Recomendación número 2) pueda concretarse en primer semestre del 2011, de esta manera las Instituciones puedan realizar su Plan Estratégico, lograr la aprobación del Plan Operativo en el segundo semestre del 2011 y empezar el plan de Implementación del sistema de Gestión de Seguridad de la Información (SGSI) utilizando la Metodología PDCA durante el 2012 contando para ello con la asesoría del Grupo Técnico de Apoyo.

Paralelamente al proceso de Implementación se tiene previsto por parte de la ONGEI la creación del organismo Auditor y la elaboración del plan de auditorías del programa de implementación de la Norma en las Instituciones, se estima que puede empezar las primeras auditorías a partir de enero del 2012.

Los resultados de los mismos se podrá publicar a partir del segundo semestre del 2013 para culminar con el informe de evaluación de los avances armonizados con los planes del Proyecto de Gobierno Electrónico, la Agenda Digital Peruana y el CEPLAN.

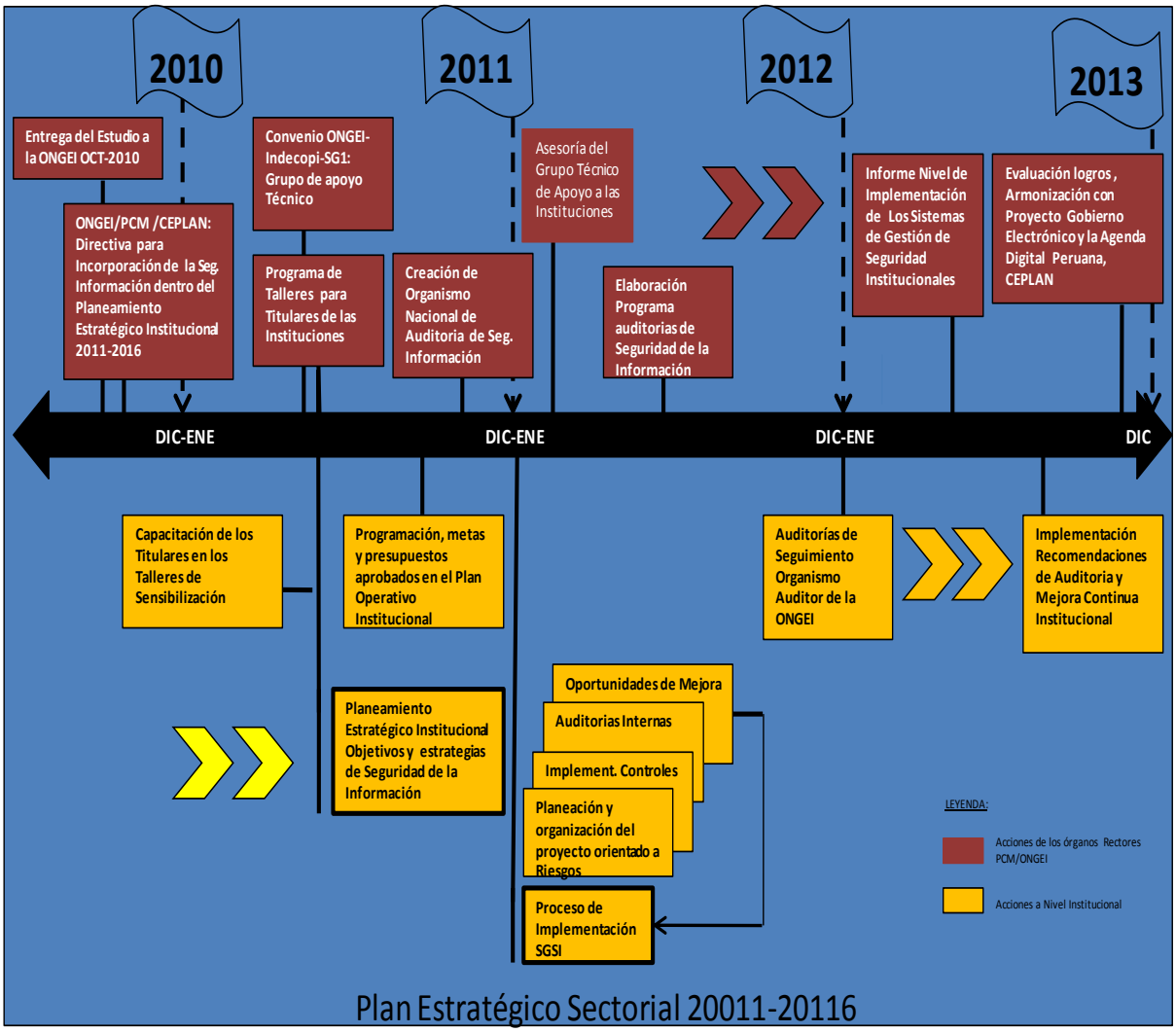

Grafico 37. **Línea de Tiempo para las líneas de acción de las Recomendaciones**

5.4 Sugerencia para futuros estudios

El presente estudio ha mostrado e identificado los factores inhibidores en la implementación de la Norma Técnica de Seguridad de la Información en los Organismos Públicos Descentralizados, también se ha comprobado que el proceso de implementación del Sistema de Gestión de seguridad basado en la Norma está en su etapa inicial por lo que proponemos como temas potenciales de estudio futuro:

Un estudio comparativo de prioridad y nivel de madurez logrado en la implementación de la NTP ISO 9000 y norma NTP ISO/IEC 17799 en la administración pública, sería importante para determinar si existen otras causas indirectas que se contrapone al acortamiento de los plazos en la implementación de la norma de Seguridad, su posible integración debido a la sinergia que se pueda generar entre los mismos.

Indicadores de Gestión para medir la efectividad de las implementaciones de los Sistemas de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 17799 en la administración pública.

Un estudio del nivel de entendimiento e interpretación del plan de acción de la Agenda Digital Peruana y el Gobierno Electrónico por parte de los Titulares de la Administración Pública.

REFERENCIAS

Al-Hamdani Wasim A. (2006). *Assessment of Need and Method of Delivery for Information Security Awareness Program Division of Computer and Technical Sciences*. Kentucky State University Frankfort. Recuperado el 15 de Agosto 2009 desde http://portal.acm.org/citation.cfm?id=1231069.

Alfawaz, S., May, L., & Mohanak, K. (2008). *E-government security in developing countries: A managerial conceptual framework.* Recuperado el 24 de mayo de 2009 desde http://www.irspm2008.bus.qut.edu.au/papers/documents/pdf/Alfawaz%20-%20E-government%20security%20in%20developing%20countries%20-%20IRSPM%20-%202008.pdf

Caralli, R., A. (2004). *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management.* Recuperado el 23 Mayo de 2009 desde *http://www.sei.cmu.edu/library/abstracts/reports/04tr010.cfm*

Calder, A., Watkins, S. (2008). IT Governanace: *A Manager's Guide to Data Security and ISO27001/ISO 27002*, 4th Edition. Recuperado el 30 de mayo de 2009 desde http://acm.books24x7.com/viewer.asp?bookid=28468&chunkid=952046549

Comisión Multisectorial para el Desarrollo de la Sociedad de la Información Multisectorial CODESI (2005) .*Mesa de Trabajo N°5 Gobierno Electrónico*, Recuperado el 27 de Noviembre, 2005 desde http://www.cpsr-peru.org/si/politicas/finalmesa5.pdf

Cumbre Mundial de la Sociedad de la Información (2005): *Agenda de Túnez para la sociedad de la información*. Recuperado 15 de Noviembre, 2007 desde http://www.itu.int/wsis/dcs2/tunis/ off/6rev1-es.html.Conkling, W. R. &

Hamilton, Jr J. A. (2008). *The importance of information security spending: an economic approach.* Recuperado el 16 de Mayo de 2009 desde http://delivery.acm.org/10.1145/1410000/1400590/p293-conkling.pdf?key1=1400590&key2=5618743521&coll=guide&dl=guide&cfid=52699252&cftoken=1680800

Ernst & Young's (2008). *Moving beyond compliance Ernst & Young's 2008 Global Information Security Survey.* Recuperado el 23 mayo de 2009 desde *http://www.ey.com/Publication/vwLUAssets/GISS_2008/$FILE/GISS2008.pdf*

European Network and Information Security Agency (ENISA) (2008). *The new users' guide: How to raise information security awareness.* Recuperado el 17 de Mayo de 2009 desde *http://www.enisa.europa.eu*

Farahmand, F., Navathe, S., B., Sharp, G., P., Enslow, P., H. (2003). *Managing Vulnerabilities of Information Systems to Security Incidents.* Recuperado el 5 de Agosto de 2009 desde *http://delivery.acm.org/10.1145/950000/948050/p348-fahramand.pdf?key1=948050&key2=2309202521&coll=acm&dl=acm&cfid=50127667&cftoken=78378071*

Gobierno de España Ministerio de Administraciones Públicas (2007). Normalización en seguridad de las tecnologías de la información. Recuperado el 24 de mayo de 2009 desde http://www.csae.map.es/csi/pdf/normalizacion.pdf

Instituto Nacional de Tecnologías de la Comunicación (2008), *Conceptos de un SGSI* Recuperado el 28 de Julio 2008 desde. https://sgsi.inteco.es/index.php/es/conceptos-de-un-sgsi

Instituto Nacional de Tecnologías de la Comunicación (INTECO) (s.f). *Impulso a la Implementación y certificación de SGSI en la Pymes*. Recuperado el 17 de mayo de 2009 desde *https://sgsi.inteco.es/index.php/conceptos-de-un-sgsi*

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (2009). *Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias.* Recuperado el 01 de Junio, 2009 desde.

http://www.indecopi.gob.pe/destacado-reglamentos-comisiones-crt-pres.jsp
International Organization for Standardization ISO (2005). *State-of-the-art information security management systems with new ISO/IEC 27001:2005 standard.* Recuperado el 20 de Mayo, 2009 desde *http://www.iso.org/iso/pressrelease.htm?refid=Ref976*

Jan Yestingsmeier, J., & Steve Guynes, S., (1982). *Personnel considerations in information systems security.* Recuperado el 5 de mayo de 2009 desde http://delivery.acm.org/10.1145/1060000/1058396/p23-yestingsmeier.pdf?key1=1058396&key2=6532202521&coll=ACM&dl=ACM&CFID=50119671&CFTOKEN=87752569

Jinx P. Walton, (2002). *Developing an enterprise information security policy.* Recuperado el 5 de Mayo de 2009 desde *http://delivery.acm.org/10.1145/590000/588678/p153-walton.pdf?key1=588678&key2=2269743521&coll=GUIDE&dl=GUIDE&CFID=52702184&CFTOKEN=25028076*

Jyotirmoyee Bhattacharjya, Vanessa Chang *An Exploration of the Implementation and Effectiveness of IT Governance Processes in Institutions of Higher Education in Australia* Recuperado el 28 de Julio 2008 desde http://espace.lis.curtin.edu.au/archive/00001767/02/1767.pdf

Julia Allen, A. (2005). Governing for Enterprise Security. Recuperado el 23 de Mayo de 2009 desde *www.cert.org/archive/pdf/05tn023.pdf*

Koskosas, L., V., Paul, R., J. (2004). *The Interrelationship and Effect of Culture and Risk Communication in Setting Internet Banking Security Goals.* Recuperado el 16 de Mayo de 2009 desde *http://delivery.acm.org/10.1145/1060000/1052264/p341-koskosas.pdf?key1=1052264&key2=0267202521&coll=acm&dl=acm&cfid=50127667&cftoken=78378071*

Mohamed Dafir Ech-cherif el Kettani (2008) . NCSec – A National Cyber Security Referential for the Development of a Code of Practice in National Cyber Security Management. Recuperado el 24 de mayo 2009 desde: http://delivery.acm.org/10.1145/1510000/1509174/p373-el_kettani.pdf?key1=1509174&key2=8332613521&coll=GUIDE&dl=ACM&CFID=52095538&CFTOKEN=51036848

Naciones Unidas (2005) Junta de Comercio y Desarrollo Comisión de la Empresa, la Facilitación de la Actividad Empresarial y el Desarrollo *Conferencia de las Naciones Unidas sobre comercio y desarrollo.* Recuperado el 26 de Julio, 2009 desde *http*://www.unctad.org/sp/docs/c3d74_sp.pdf

National Institute of Standards and Technology (2002). *Risk Management Guide for Information Technology Systems* Special Publication 800-30

Partida, A, & Ezingeard, J. (2007). *Critical success factors and requirements for achieving business benefits from information security.* Recuperado el 26 de Abril, 2009 desde *http://www.iseing.org/emcis/EMCIS2007/emcis07cd/EMCIS07-PDFs/687.pdf*

PCM/ONGEI (Ed.). (2005). *Plan de Desarrollo de la sociedad de la Información en el Perú: La Agenda Digital Peruana*. Lima:ONGEI.

PCM/ONGEI: *Política de Seguridad- Modelo Simplificado*. Recuperado 15 agosto de 2009, desde http://www.pecert.gob.pe/index.php?option=com_content&view=article&id=44&Itemid=56&limitstart=2

PCM (Ed) (2008). *Seguridad de la Información: Centro de consulta e investigación sobre seguridad de la información*. Recuperado el 26 de Julio, 2008 desde. http://www.ongei.gob.pe/seguridad/seguridad2_archivos/Lib5158/Libro.pdf

Presidencia de Consejo de Ministros- Gobierno del Perú- ONGEI (2004) *Resolución Ministerial No. 224-2004-PCM. Aprobación de la Norma Técnica Peruana NTP-ISO/IEC 17799.*

Preda, P., Cuppens, F., Cuppens-Boulahia, N., Alfaro, J., G., Toutain, L., Elrakaiby, Y., (2009). *Semantic Context Aware Security Policy Deployment* Recuperado el 5 de Agosto de 2009 desde *http://delivery.acm.org/10.1145/1540000/1533092/p251-preda.pdf?key1=1533092&key2=6464202521&coll=acm&dl=acm&cfid=50119671&cftoken=87752569*

The IT Governance Institute (ITGI, 2008) *IT Governance Global Status Report 2008* Recuperado el 20 de Mayo, 2009 desde *http://www.pwc.com/en_BE/be/multimedia/it-governance-global-statut-report-pwc-08.pdf*

Rafael, C., Alessio, D., Víctor, D., Horacio, D. (2004) Concientización en Seguridad de la Información Facultad de Ingeniería, Departamento de Sistemas y Computación Universidad de los Andes – Bogotá, Colombia. Recuperado el 24 de mayo de 2009 desde http://www.criptored.upm.es/guiateoria/gt_m142r.htm

Richard L. Rollason-Reese (2003). *Incident handling: an orderly response to unexpected events.* Eastern Connecticut State University. Recuperado el 21 de mayo, 2009 desde *http://portal.acm.org/results.cfm?coll=GUIDE&dl=ACM&CFID=51247843&CFTOKEN=29146142*

Rodewald, G. (2005) *Aligning Information Security Investments with a Firm's Risk Tolerance.* Recuperado el 16 de Mayo de 2009 desde *http://delivery.acm.org/10.1145/1110000/1107654/p139-rodewald.pdf?key1=1107654&key2=2618202521&coll=acm&dl=acm&cfid=50127667&cftoken=78378071*

Rollason-Reese, R., L. (2003). *Incident Handling: An Orderly Response to Unexpected Events.* Recuperado el 17 de mayo de 2009 desde *http://portal.acm.org/citation.cfm?id=947469.947496&coll=acm&dl=acm&cfid=50127667&cftoken=78378071*

Suhair Hafez Amer, S. H & Hamilton, J.,A.,Jr. ,(2008).*Understanding security architecture.* Recuperado el 5 de Mayo de 2009 desde *http://delivery.acm.org/10.1145/1410000/1400596/p335-amer.pdf?key1=1400596&key2=4352202521&coll=acm&dl=acm&cfid=50119671&cftoken=87752569*

Savola, R., M. (2007).*Towards Taxonomy for Information Security Metrics.* Recuperado el 17 de mayo de 2009 desde *http://delivery.acm.org/10.1145/1320000/1314266/p28-savola.pdf?key1=1314266&key2=2229202521&coll=acm&dl=acm&cfid=50127667&cftoken=78378071*

Saucedo, G., M. (2007). II Encuesta Nacional sobre Seguridad Informática en México – 2008 – Análisis de resultados y comparativo 2007-2008 - Recuperado el 23 de Mayo de 2009 desde *http://www.acis.org.co/fileadmin/Revista_105/EMexico.pdf*

Saleh, M, S., Abdullah Alrabiah, A., & Saad Haj Bakry, S., B. (2007). Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach. Recuperado el 24 de mayo de 2009 desde http://delivery.acm.org/10.1145/1220000/1217443/p85saleh.pdf?key1=1217443&key2=4205843521&coll=GUIDE&dl=GUIDE&CFID=53878073&CFTOKEN=31524173

Stevenson , B. R, Gordon W. Romney, G., W. (2004). Teaching security best practices by architecting and administering an IT security lab . Recuperado el 30 de mayo 2009 desde ACM: http://delivery.acm.org/10.1145/1030000/1029578/p182-stevenson.pdf?key1=1029578&key2=4630323521&coll=Portal&dl=ACM&CFID=52228659&CFTOKEN=24610330

SaadSaleh AlAboodi, S., S (2006) A New Approach for Assessing the Maturity of Information Security Master's thesis for Hull University, UK. Recuperado el 30 de mayo de 2009 desde http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=34805&TEMPLATE=/ContentManagement/ContentDisplay.cfm

The National Institute of Standards and Technology NIST (2006). *Information Security Handbook: A Guide for Managers.* Recuperado el 5 de Agosto de 2009 desde *http://csrc.nist.gov/publications/nistir/ir7359/CSD_ExecGuide-booklet.pdf*

Wolcott Group (s.f.) **.**Free ISO 27001 Online Self-Assessment on Information Security. Recuperado el 30 de mayo del 2009 desde https://benchmark.wolcottgroup.com/baseline/baseline.nsf/ISO27001AssessmentPreview03.pdf?OpenFileResource

Wasim A. Al-Hamdani (2006).*Assessment of Need and Method of Delivery for Information Security Awareness Program* .Recuperado el 16 de Mayo de 2009 desde *http://delivery.acm.org/10.1145/1240000/1231069/p102-al-hamdani.pdf?key1=1231069&key2=2317202521&coll=acm&dl=acm&cfid=50127667&cftoken=78378071*

Whitman Michael E., Caylor J. (2005) *Rebuilding the Human Firewall* Information security curriculum development Proceedings of the 2nd annual conference on Information security curriculum development , recuperado el 15 de agosto de 2009 desde http://portal.acm.org/citation.cfm?id=1107646

ANEXOS

ANEXO 1

Comisiones de Seguridad UIT y Datos sobre ISO 27001/ NTP ISO 17799

Tabla 17. **Lista de Comisiones de Estudio y Cuestiones relativas al tema de la seguridad UIT**

Elementos de seguridad del UIT-T

Marco de arquitectura de seguridad

- X.800 – Arquitectura de seguridad
- X.802 – Modelo de seguridad de capas más bajas
- X.803 – Modelo de seguridad de capas superiores
- X.805 – Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo
- X.810 – Marcos de seguridad para sistemas abiertos: Visión general
- X.811 – Marcos de seguridad para sistemas abiertos: Marco de autenticación
- X.812 – Marcos de seguridad para sistemas abiertos: Marco de control de acceso
- X.813 – Marcos de seguridad en sistemas abiertos: Marco de no rechazo
- X.814 – Marcos de seguridad para sistemas abiertos: Marco de confidencialidad
- X.815 – Marcos de seguridad para sistemas abiertos: Marco de integridad
- X.816 – Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad

Protocolos

- X.273 – Protocolo de seguridad de la capa de red
- X.274 – Protocolo de seguridad de la capa de transporte

Seguridad en la retransmisión de tramas

- X.272 – Compresión de datos y privacidad en las redes con retransmisión de tramas

Técnicas de seguridad

- X.841 – Objetos de información de seguridad
- X.842 – Directrices para el uso y gestión de servicios a tercera parte confiable
- X.843 – Especificación de servicios de tercera parte confiable para soportar la aplicación de firmas digitales

Servicios de directorio y autenticación

- X.500 – Visión de conjunto de conceptos, modelos y servicios
- X.501 – Modelos
- X.509 – Marco para los certificados de claves públicas y de atributos
- X.519 – Especificaciones de protocolo

Seguridad de gestión de redes

- M.3010 – Principios para una red de gestión de las telecomunicaciones
- M.3016 – Visión general de la seguridad en la red de gestión de las telecomunicaciones
- M.3210.1 – Servicios de gestión de red de gestión de las telecomunicaciones para la seguridad de las IMT-2000
- M.3320 – Marco de los requisitos de gestión para la interfaz X de la RGT
- M.3400 – Funciones de gestión de la red de gestión de las telecomunicaciones

Gestión de sistemas

- X.733 – Función señaladora de alarmas
- X.735 – Función control de ficheros registro cronológico
- X.736 – Función señaladora de alarmas de seguridad
- X.740 – Función de pista de auditoría de seguridad
- X.741 – Objetos y atributos para el control de acceso

Facsímil

- T.30 Anexo G – Procedimientos para la transmisión segura de documentos por facsímil grupo 3 mediante la utilización de los sistemas HKM y HFX
- T.30 Anexo H – Seguridad en facsímil del grupo 3 basada en el algoritmo RSA
- T.36 – Capacidades de seguridad para su utilización con terminales facsímil del grupo 3
- T.503 – Perfil de aplicación de documento para el intercambio de documentos facsímil del grupo 4
- T.563 – Características de terminal para aparatos facsímil del grupo 4

Sistemas de televisión y cable

- J.91 – Métodos técnicos para asegurar la privacidad de las transmisiones internacionales de televisión a larga distancia
- J.93 – Requisitos del acceso condicional en la distribución secundaria de televisión digital por sistemas de televisión por cable
- J.170 – Especificación de seguridad de IPCablecom

Comunicaciones multimedios

- H.233 – Sistemas de confidencialidad para servicios audiovisuales
- H.234 – Sistema de gestión de claves de criptación y de autenticación para servicios audiovisuales
- H.235 – Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)
- H.323 Anexo J – Sistemas de comunicación multimedios basados en paquetes – Seguridad para el anexo F/H.323 (Tipos de punto extremo simples)
- H.350.2 – Arquitectura de servicios de directorio para H.235
- H.530 – Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510

Las Recomendaciones del UIT-T pueden consultarse en el sitio de la UIT en la red: http://www.itu.int/publications/bookshop/how-to-buy.html (en este sitio figura también información sobre el acceso gratuito a un número limitado de Recomendaciones del UIT-T).

Tabla 18. **Certificaciones ISO 27001 en el mundo.**

Japan	3572	Philippines	15	Peru	3
India	490	Pakistan	14	Portugal	3
UK	448	Iceland	13	Argentina	2
Taiwan	373	Saudi Arabia	13	Belgium	2
China	373	Netherlands	12	Bosnia Herzegovina	2
Germany	138	Singapore	12	Cyprus	2
Korea	106	Indonesia	11	Isle of Man	2
USA	96	Bulgaria	10	Kazakhstan	2
Czech Republic	85	Norway	10	Morocco	2
Hungary	71	Russian Federation	10	Ukraine	2
Italy	61	Kuwait	9	Armenia	1
Poland	56	Sweden	9	Bangladesh	1
Spain	43	Colombia	8	Belarus	1
Malaysia	39	Iran	8	Denmark	1
Ireland	37	Bahrain	7	Dominican Republic	1
Austria	35	Switzerland	7	Kyrgyzstan	1
Thailand	34	Croatia	6	Lebanon	1
Hong Kong	32	Canada	5	Luxembourg	1
Romania	30	South Africa	5	Macedonia	1
Australia	29	Sri Lanka	5	Mauritius	1
Greece	28	Vietnam	5	Moldova	1
Mexico	24	Lithuania	4	New Zealand	1
Brazil	23	Oman	4	Sudan	1
Turkey	21	Qatar	4	Uruguay	1
UAE	20	Chile	3	Yemen	1
Slovakia	19	Egypt	3		
France	18	Gibraltar	3		
Slovenia	16	Macau	3	**Total**	**6573**

Fuente: **HTTP://WWW.ISO27001CERTIFICATES.COM/**

Tabla 19. **Cuadro de Entidades y porcentaje del proceso de implementación de la Norma NTP-ISO/IEC 17799**

CUADRO N° 08:
PROCESO DE IMPLEMENTACION DE LA NORMA ISO 17799 - BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

Poderes, sectores y Gobiernos Regionales y Locales	Total de Entidades		SI		No	
	N°	%	N°	%	N°	%
I.- PODER EJECUTIVO						
I.1.- SECTORES						
Presidencia del Consejo de Ministros	14	100	6	42.86	8	57.14
Agricultura	4	100	1	25.00	3	75.00
Comercio Exterior y Turismo	2	100	2	100.00		
Defensa	14	100	7	50.00	7	50.00
Economía y Finanzas	16	100	7	43.75	9	56.25
Educación y Cultura	5	100	3	60.00	2	40.00
Energía y Minas	3	100	3	100.00		
Interior	5	100	3	60.00	2	40.00
Justicia	4	100	3	75.00	1	25.00
Mujer y Desarrollo Social	6	100	2	33.33	4	66.67
Producción	4	100	2	50.00	2	50.00
Relaciones Exteriores	1	100	1	100.00		
Salud	3	100	3	100.00		
Transportes y Comunicaciones	2	100			2	100.00
Vivienda, Construcción y Saneamiento	5	100	2	40.00	3	60.00
OPDs en Regiones	14	100	3	21.43	11	78.57
I.2.- EMPRESAS ESTATALES	31	100	17	54.84	14	45.16
II.- PODER JUDICIAL	**2**	**100**	**2**	**100.00**		
III.- PODER LEGISLATIVO	**1**	**100**	**1**	**100.00**		
IV.- GOBIERNOS REGIONALES						
Gobiernos Regionales	199	100	15	7.54	184	92.46
V.- GOBIERNOS LOCALES						
Gobiernos Locales	168	100	25	14.88	143	85.12
Empresas Municipales	38	100	6	15.79	32	84.21
VI.- ORGANISMOS AUTONOMOS						
VI.1.- Organismos Autónomos	**9**	**100**	**5**	**55.56**	**4**	**44.44**
VI.2- Universidades	**26**	**100**	**5**	**19.23**	**21**	**80.77**
NACIONAL	**576**	**100**	**124**	**21.53**	**452**	**78.47**

FUENTE: VI ENRIAP, Nov-Dic. 2007, Oficina Nacional de Gobierno Electrónico e Informática, ONGEI

ANEXO 2

DISEÑO ENCUESTA IMPLEMENTACIÓN DE LA NTP-ISO/IEC 17799- PCM/ONGEI
Organismos Públicos Descentralizados Adscritos a la Presidencia del Consejo de Ministros

Instrucciones:

La presente encuesta, está dirigida a los titulares de cada institución su utilidad será de gran importancia para el desarrollo del proyecto de Gobierno Electrónico del país por lo que se le solicita responder con la mayor objetividad e imparcialidad posible, agradeceremos su valioso aporte y colaboración.

La encuesta tiene 3 Partes:

I. Sobre los Dominios de Control de la Norma Técnica Peruana NTP-ISO/IEC 17799.
II. Sobre el Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información basado en la Norma.
III. Sobre el grado de influencia de los Factores Críticos en la implementación de la Norma.

Las respuestas a estas preguntas, nos permitirá tener una visión compartida y un rumbo de futuro claro, real y conocer en forma objetiva:

1) ¿Dónde Estamos? , que dificultades hay ?

2) Luego del análisis ¿A dónde queremos ir?

3) ¿Cómo llegar a donde queremos ir? En relación con la Seguridad de la Información en el Sector.

DATOS GENERALES

Complete los siguientes datos:

Nombre de la Institución:

……..……..

Nombre del titular de la Institución:

……..……..

Cargo:

……

Nombre del que responde la encuesta:

(*)……

(*) En caso de que el titular por alguna razón no sea la persona que contesta la encuesta

Cargo:

…….…….

Correo electrónico:

…….…….

Cualquier coordinación al teléfono: 2247800 anexo 1432, o al correo amarino@indecopi.gob.pe.

CUESTIONARIO

I. Sobre los Dominios de Control de la Norma Técnica Peruana NTP-ISO/IEC 17799

Lea las siguientes definiciones sobre los dos temas a evaluar a) Agrega valor a la Institución, b) Nivel de madurez de la implementación por Dominio, y marque sus respuestas en el cuadro de preguntas para los 11 Dominios.

a) Agrega valor a la institución

(1) Agrega poco o nada de valor: Este control no se aplican a los procesos y es percibido como que tienen poco o ningún impacto en las operaciones de la Institución.

(2) Algo de valor: La mayoría de la institución no reconoce que tenga algún valor, pero provee algo de valor donde es usado. Por lo tanto este control está siendo usado solo en partes de la institución, aunque no en forma consistente.

(3) Provee valor: Este control provee valor a la mayoría de las áreas de la Institución, pero puede no estar formalmente reconocido o documentado.

(4)Provee de Valor Adicional: Este control es reconocido como que agrega valor a los procesos de negocio, a través del incremento de la eficiencia de la seguridad. Este control es requerido en toda la organización por política de seguridad, pero aún no está completamente implementado.

(5) Crítico para el éxito de la Institución: Este control es reconocido como crítico y afecta directamente la rentabilidad o efectividad del servicio, y está relacionado con la política General, la política de seguridad o requerimientos legales.

b) Nivel de madurez de la implementación por Dominio

(1)No implementado: En ningún proceso de la institución

(2)Inicial: Se reconoce que el problema de seguridad existe y la necesidad de abordarlo pero no se ha formalizado ni documentado para su implementación.

(3) En proceso de desarrollo: Los procesos de seguridad aún están en desarrollo, fundamentalmente en base al conocimiento del personal, con limitada documentación.

(4) Definido: Los procedimientos de seguridad han sido estandarizados, documentados y comunicados a través de capacitación. Falta reforzar que se cumpla con los procedimientos, el monitoreo y mediciones son todavía limitadas.

(5) Gestionado: Se puede monitorear y medir el cumplimiento de los procedimientos. Se usan herramientas automatizados aunque en forma limitada o fragmentada.

(6)Optimizado: Los procesos se han refinado para cumplir con las mejores prácticas basados en la mejora continua.

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
1	Política de Seguridad	1.- La política de la seguridad de la información existe está vigente, y alineado con las metas y objetivos de la Institución											
		2.-La Política de la Seguridad de la Información ha sido comunicado a todas las partes involucradas											
		3.-La Política de la Seguridad de la Información es revisada en forma periódica o cuando se produce un cambio significativo y ha sido validado por una organización independiente											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
2	Organiza-ción de la seguridad de la Información	1.-Todas las responsabilidades de la Seguridad de la Información están claramente definidas por los representantes con roles y funciones de trabajo relevantes											
		2.-Los Objetivos de control, controles, políticas, procesos, tecnología y procedimientos son revisados independientemente en forma periódica o cuando se produce un cambio significativo en la infraestructura de seguridad.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
		3.-Los Acuerdos con terceros sobre el acceso, procesamiento, comunicación o administración de la información o instalaciones de la Institución cubren los requerimientos relevantes de seguridad y regulatorias. Adicionalmente estos acuerdos son revisados periódicamente para asegurar que están vigentes y operativos.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
3	Gestión de Activos	1.- Todos los activos de la Institución están claramente identificados y existe un inventario actualizado de todos activos críticos actualizados. Este inventario incluye nombre del activo, propósito, impacto para la Institución y propietario.											
		2.- Se han implementado reglas para un aceptable uso de la información y los activos de información están identificados y documentados. Estas reglas han sido efectivamente comunicadas a todos los empleados.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
		3.- La información ha sido clasificada en términos de su valor, requerimientos legales, sensibilidad y criticalidad para la Institución.											
4	Seguridad de Recursos Humanos	1.-Los roles de Seguridad y responsabilidades de los empleados, contratistas, vendedores y usuarios de terceros están definidas y documentadas en concordancia con las políticas de la Institución, requerimientos legales y otras políticas institucionales.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
		2.-Todos los empleados de la Institución y donde sea relevante, contratistas y usuarios de terceros, reciben un entrenamiento de refrescamiento y actualización sobre las políticas institucionales, requerimientos legales y procedimientos relevantes a sus funciones de trabajo y responsabilidades relacionadas con la seguridad.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
5	Seguridad física y ambiental	1.-Protección física contra daños de Fuego, inundaciones, terremotos, explosión, guerras civiles, y otras formas de desastres naturales o causados por humanos están implementados y operativos. Adicionalmente las Áreas seguras están protegidas por controles de entrada apropiados para asegurar que sólo personal autorizado tiene permitido el acceso.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
6	Gestión de las Comunica-ciones y Operacio-nes	1.-La red está adecuadamente administrada y controlada, y está protegida de amenazas. La protección está dada para los sistemas, aplicaciones, dispositivos de red, información almacenada y en tránsito.											
		2.-Las obligaciones críticas y áreas de responsabilidad están documentadas y segregadas para reducir oportunidades de fraude y otros usos no autorizados/ mal uso no intencional de los activos de la Institución.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
		Esto es particularmente crítico in Finanzas, IT y seguridad.											
7	Control de acceso	1.-Los derechos de acceso de todos los empleados, contratistas y terceros a los activos de la Institución, ambos físico e información, están controlados y monitoreados a través de procesos documentados y operativos de administración de identidad o gestión de usuarios.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
8	Adquisición desarrollo y Mant. De Sistemas de Información	1.- Los requisitos del sistema de seguridad de la información y procesos para implementar la seguridad son integrados en las etapas iniciales de los proyectos de los sistemas de información.											
		2.-Si los productos son comprados se realiza una prueba formal y un proceso de adquisición. Los contratos con el proveedor deben especificar los requisitos de seguridad.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
9	Gestión de Incidencias de Seguridad de la Información	1.-Todos los empleados, contratistas, y usuarios terceros de los sistemas de información y servicios registran y reportan cualquier sospecha de seguridad o debilidad en los sistemas y servicios. Existe un proceso documentado y operacional para gestionar los incidentes de seguridad.											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
10	Gestión de la Continui-dad del Negocio	1.- Un proceso administrado ha sido desarrollado, probado y mantenido para la continuidad del Negocio a través de la institución. Incluye los requerimientos necesarios de seguridad de la información para que el negocio de la Institución continúe en una forma segura y protegida.											
11	Cumpli-miento	1.-Todos los estatutos relevantes, requerimientos contractuales y regulatorios y todos los alcances de la institución para cumplir estos requerimientos están											

			a. Agrega Valor a la Institución					b. Nivel de madurez de la Implementación por dominio					
			(1) Poco o nada de valor	(2) Algo de valor	(3) Provee valor	(4)Provee Valor Adicional	(5) Critico para el éxito de la Institución	(1) No Implementado	(2) Inicial	(3) En proceso de desarrollo	(4) Definido	(5) Gestionado	(6) Optimizado
No Dominio	Descripción del Dominio	Pregunta de la encuesta											
		explícitamente definidos, documentados, y mantenidos al día para cada sistema de información y la institución.											
		2.-Los sistemas de información y sus procesos asociados son chequeados en forma periódica para asegurar que no hay desviaciones en el cumplimiento con los requerimientos voluntarias y mandatorios de la Institución.											

II. Sobre el Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma. Marcar con una x o consignar los datos numéricos según corresponda.

	SI	NO
1. Su institución ha iniciado el proceso de implementación de la NTP-ISO/IEC 17799?		

Si es SI: Indique fecha de:

Inicio:…….FIN:…….Continúa:……

Si ha marcado NO pase a la pregunta 6.

2.- Que metodología ha adoptado para la gestión y evaluación de riegos? Marcar en el recuadro:

a) OCTAVE	
b) MEHARI	
c) ISO TR 13335	
d) BS 7799 Parte 3	
d) Otra (especificar):……..	
e) No se ha iniciado el proceso	

3.- Como resultado de la evaluación de riesgos su institución tiene definido el alcance del SGSI ?

a) Procesos identificados como críticos (indicar No. de procesos priorizados)……..

b) Porcentaje de riesgos identificado como:

Alta…….. Media…….. Baja…….No evaluados…….

c) Controle (Indicar el No de controles de la norma seleccionados en total)……..

d) La definición y evaluación está en proceso

e) No se ha iniciado el proceso de definición y evaluación

4.-Si su institución ha adoptado el modelo simplificado de implementación recomendado por la ONGEI o cualquier otro, marque el nivel de implementación alcanzado, y valore el grado de dificultad que ha experimentado de 0 a 5 en las etapas y sus respectivas actividades.

	Nivel de Implementación a la fecha						Grado de dificultad en implementación				
Proceso de implementación de la NTP-ISO/IEC 17799	No implementado	Inicial	desarrollo	Definido	Gestionado	Optimizado	(1) No hay dificultad	(2) algo de dificultad	dificultad	(4) alta dificultad	(5) Muy alta dificultad
1. ETAPA I											
1.1. Análisis e interpretación de los requerimientos de seguridad en base a la misión, visión y objetivos de la organización											
1.2. Identificación de los recursos (activos) dentro de los procesos de la organización											
2. ETAPA II											
2.1. Establecimiento de la Política de Seguridad de la organización											
2.2. Efectuar un análisis de riesgos											
2.3. En base a los controles establecidos para cada dominio de la Norma, establecer la Brecha (Lo que se tiene y lo que falta implementar) SOA											
3. ETAPA III											
3.1. Establecimiento del documento del plan a 1, 2 o 3 años											
3.2. Implementación del Plan de Seguridad dentro del POI											
4. ETAPA IV											
4.1. Política de Seguridad											
4.2. Análisis de riesgos											
4.3. Brecha de lo implementado y lo que falta por implementar											
4.4. Plan de Seguridad de la Información (reflejado en el POI)											

5.- Si su respuesta en la pregunta 4 fue NO, especifique el Modelo adoptado:…….

6.-Señale (Marcar con una X) en orden de importancia (1 a 8 , siendo 1 el más importante) los factores principales que dificultan el cumplimiento con los plazos de implementación de la Norma dadas por la PCM:	1	2	3	4	5	6	7	8
a) Falta de Personal especializado en Seguridad de la información								
b)Presupuesto Insuficiente o no asignado								
c) Falta un entendimiento cabal sobre la Seguridad de la información por parte de la alta dirección para apoyar con mayor efectividad estas iniciativas								
d)Falta de capacitación y concienciación del personal								
e) Dificultad para alinear la seguridad de la información con los objetivos estratégicos de la institución (No se percibe el beneficio de la seguridad de la información)								
f) Dificultad en la gestión del proyecto y obtener los resultados esperados								
g) No se ha formalizado la creación del Área de Seguridad de la información y el responsable dentro de la institución								
h) Dificultad para cambiar la cultura organizacional orientado a la seguridad de la información (Resistencia al cambio)								
i) Otros: Especificar…….								

7.- Según su opinión la responsabilidad de la seguridad de la información en una organización es:

a) De la Alta dirección	
b) De la Gerencia de Sistemas	
c) Del Gerente o jefe de área de la seguridad de la información	
d) Del Gerente General	
e) De todos los empleados	
f) Otros: Especificar……	

8.- Según su opinión para efectivizar el cumplimiento de la implementación de la norma la ONGEI: (Puede marcar más de uno)

a) Debería realizar una auditoría de verificación de cumplimiento	
b) Debería aplicar sanciones a los que incumplen	
c) Debería establecer premios de cumplimiento	
d)Debe apoyar con consultorías especializadas	
e) Otros: Especificar……	

III. Sobre el grado de influencia de los Factores Críticos en la implementación de la Norma

1.-Según su experiencia valore el grado de influencia de cada uno de los factores para la implementación de la norma (Marcar con una X en el cuadro según corresponda).

1 Ninguna influencia
2 Algo de influencia
3 Mediana influencia
4 Alta influencia
5 Muy alta influencia

	GRADO DE INFLUENCIA				
Grado de influencia de los factores críticos en la implementación de la NTP-ISO/IEC 17799	1	2	3	4	5
a) Una política, objetivos y actividades que reflejen lo objetivos de negocio de la organización					
b) Un enfoque para implantar, mantener y monitorear e improvisar la seguridad que sea consistente con la cultura de la organización					
c) El apoyo visible y el compromiso de la alta gerencia					
d) La buena compresión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo					
e) La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados					
f) la distribución de guías sobre la política de seguridad de la información y de normas a todos los empleados y contratistas					
g) Aprovisionamiento para financiar actividades de gestión de la seguridad de la información					
h) la formación y capacitación adecuadas					
i) Establecer un efectivo proceso de gestión de incidentes de la seguridad de la información					
j) Un sistema integrado y equilibrado de medidas que permita evaluar el rendimiento de la seguridad de la información y sugerir medidas.					

2.-Ud. Considera que hay otros factores más influyentes que facilitarían la implementación de la Norma en su institución...?	GRADO DE INFLUENCIA				
	1	2	3	4	5
k)					
l)					
m)					
n)					

3.- Según su apreciación , las herramientas (Seguridad de la información/Documentos/Plantillas) disponibles en el Portal de la ONGEI

a) Son muy útiles	
d) Medianamente útil	
c) Está incompleto	
d)No es aplicable	
e) Otros: Comentar brevemente:…….	

…….

ANEXO 3

TABLA DE OPERACIONALIZACION DE VARIABLES

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Nivel de valoración de la Norma por la Institución	Política de Seguridad	--	Cuestionario Semi estructurado	1) Poco o nada de valor 2) Algo de valor 3) Provee valor 4) Provee valor adicional 5) Crítico para el éxito de la Institución	Variable independiene
	Organización de la Seguridad de la Información				
	Gestión de Activos				
	Seguridad de Recursos Humanos				
	Seguridad física y ambiental				
	Gestión de las comunicaciones y operaciones				
	Control de Acceso				
	Adquisición, desarrollo y Mant. De sistemas de información				
	Gestión de incidencias de Seguridad de la Información				
	Gestión de Continuidad del Negocio				
	Cumplimiento				

TABLA DE OPERACIONALIZACION DE VARIABLES

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Grado de influencia de los Factores Críticos en la implementación de la Norma	Valoración sobre la influencia de los Factores Críticos en la implementación de la norma	Una política, objetivos y actividades que reflejen lo objetivos de negocio de la organización	Cuestionario Semi estructurado	1) Ninguna influencia 2) Algo de influencia 3) Mediana influencia 4) Alta influencia 5) Muy alta influencia	Variable Independiente
		Un enfoque para implantar, mantener y monitorear e improvisar la seguridad que sea consistente con la cultura de la organización			
		El apoyo visible y el compromiso de la alta gerencia			
		La buena compresión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo			
		La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados			
		La distribución de guías sobre la política de seguridad de la información y de normas a todos los empleados y contratistas			
		Aprovisionamiento para financiar actividades de gestión de la seguridad de la información			
		La formación y capacitación adecuadas			
		Establecer un efectivo proceso de gestión de incidentes de la seguridad de la información			

TABLA DE OPERACIONALIZACION DE VARIABLES (Cont.)

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Grado de influencia de los Factores Críticos en la implementación de la Norma	Otros factores más influyentes que facilitarían la implementación de la norma	--	Cuestionario Semi estructurado	1) Ninguna influencia 2) Algo de influencia 3) Mediana influencia 4) Alta influencia 5) Muy alta influencia	Variable Independiente
	Apreciación sobre las herramientas disponibles para la implementación de la norma en el Portal de la ONGEI	--	Cuestionario Semi estructurado	a) Son muy útiles d) Medianamente útil c) Está incompleto d)No es aplicable e) Otros	

TABLA DE OPERACIONALIZACION DE VARIABLES (Cont.)

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma	Iniciación proceso de Implementación de la NTP - ISO/IEC 17799	--	Cuestionario Semi estructurado	a) Si b) No	Variable independiente
	Metodología para la gestión y evaluación de riesgos	--	Cuestionario Semi estructurado	a)OCTAVE b) MEHARI c) ISO TR 13335 d) BS 7799 Parte 3 e) Otra f) No se ha iniciado el proceso	
	Definición del alcance del SGSI	--	Cuestionario Semi estructurado	a) No. Procesos Identificados b)Porcentaje de riesgos identificados c)Número de controles de la norma seleccionada d) La definición y evaluación está en proceso f) No se ha iniciado el proceso de definición y evaluación	

	Aplicación de la Norma NTP - ISO/IEC 17799	***ETAPA I***	Cuestionario Semi estructurado	***Nivel de Implementación***	
		* Análisis e interpretación de los requerimientos de seguridad en base a la misión, visión y objetivos de la organización		1) No implementado	
		* Identificación de los recursos (activos) dentro de los procesos de la organización		2) Inicial	

TABLA DE OPERACIONALIZACION DE VARIABLES

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma	Orden de importancia de los factores principales que dificultan el cumplimiento con los plazos de implementación de la Norma dadas por la PCM	Falta de Personal especializado en seguridad de la información	Cuestionario Semi estructurado	Ranking de 1 -- 8	Variable independiente
		Presupuesto Insuficiente o no asignado			
		Falta un entendimiento cabal sobre la seguridad de la información por parte de la alta dirección para apoyar con mayor efectividad			
		Falta de capacitación y concienciación del personal			
		Dificultad para alinear la seguridad de la información con los objetivos estratégicos de la institución			
		Dificultad en la gestión del proyecto y obtener los resultados esperados			
		Otros			

TABLA DE OPERACIONALIZACION DE VARIABLES (Cont.)

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Proceso de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma	La responsabilidad de la seguridad de la información en la organización	--	Cuestionario Semi estructurado	a) Alta Dirección b) Gerencia de Sistemas c) Gerente o jefe de área de la seguridad de la información d) Gerente General e) De todos los empleados f) Otros	Variable independiente
	Medidas para fomentar el cumplimiento de de la norma por parte de la ONGEI	--	Cuestionario Semi estructurado	a) Debería realizar una auditoría de verificación de cumplimiento b) Debería aplicar sanciones a los que incumplen c) Debería establecer premios de cumplimiento d) Debe apoyar con consultorías especializadas e) Otros	

TABLA DE OPERACIONALIZACION DE VARIABLES

Variable	Dimensión	Sub Dimensión	Indicador	Escala	Tipo de Variable
Grado de Madurez de Implementación de la Norma	Política de Seguridad		Cuestionario Semi estructurado	1) No implementado 2) Inicial 3) En proceso de desarrollo 4) Definido 5) Gestionado 6) Optimizado	Variable dependiente
	Organización de la Seguridad de la Información				
	Gestión de Activos				
	Seguridad de Recursos Humanos				
	Seguridad física y ambiental				
	Gestión de las comunicaciones y operaciones				
	Control de Acceso				
	Adquisición, desarrollo y Mant. De sistemas de información				
	Gestión de incidencias de Seguridad de la Información				
	Gestión de Continuidad del Negocio				
	Cumplimiento	--			

ANEXO 4

a) Nivel de valoración y de madurez de la implementación por dominio

Tabla II

Dominio	Promedio de Valoración por Dominio	Valoración	Promedio de Nivel de madurez por Dominio	Nivel de madurez
Política de Seguridad	3,3	Provee valor	3,1	En proceso de desarrollo
Organización de la seguridad de la información	3,4	Provee valor	3,2	En proceso de desarrollo
Gestión de Activos	3,5	Provee valor	3,3	En proceso de desarrollo
Seguridad de Recursos Humanos	3,5	Provee valor	3,1	En proceso de desarrollo
Seguridad física y ambiental	3,5	Provee valor	3,5	En proceso de desarrollo
Gestión de las Comunicaciones y Operaciones	3,9	Provee valor adicional	3,8	Definido
Control de acceso	3,7	Provee valor adicional	3,4	En proceso de desarrollo
Adquisición desarrollo y Mantenimiento de Sistemas de Información	3,6	Provee valor adicional	3,6	Definido
Gestión de incidencias de Seguridad de la Información	3,5	Provee valor	2,7	En proceso de desarrollo
Gestión de la Continuidad del Negocio	3,9	Provee valor adicional	2,9	En proceso de desarrollo
Cumplimiento	3,5	Provee valor	3,1	En proceso de desarrollo
Promedio Global	**3,6**	**Provee valor adicional**	**3,2**	**En proceso de desarrollo**

II. Sobre el proceso de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma.

Su institución ha iniciado el proceso de implementación de la NTP-ISO/IEC 17799

Ítem	n	%
Si	7	43,8
No	9	56,3
Total	16	100,0

Etapa del proceso de implementación

Ítem	n	%
Continua	6	100,0
No contestaron	1	

¿Qué metodología ha adoptado para la gestión y evaluación de riesgos?

Ítem	n	%
BS 7799 Parte 3	3	60,0
Otra	1	20,0
No se ha iniciado el proceso	1	20,0
Total	5	100,0
No contestaron	2	

Como resultado de la evaluación de riesgos ¿su institución tiene definido el alcance del SGSI?

Ítem	n	%
Porcentaje de riesgos identificado como	1	6,3
Controles	1	6,3
La definición y evaluación está en proceso	3	18,8
No se ha iniciado el proceso de definición y evaluación	2	12,5
Total	7	43,8

Nivel de Implementación a la fecha

Etapa I.1 Análisis e interpretación delos requerimientos de seguridad en base a la misión, visión y objetivos de la organización

Nivel de implementación hasta la fecha	n	%
En proceso de desarrollo	2	33,3
Definido	2	33,3
Gestionado	2	33,3
Total	6	100,0
No contestaron	1	

Etapa I.2 Identificación de los recursos (activos) dentro de los procesos de la organización

Nivel de implentacion hasta la fecha	n	%
No implementado	1	16,7
Definido	3	50,0
Gestionado	2	33,3
Total	6	100,0
No contestaron	1	

Etapa II.1 Establecimiento de la política de seguridad de la organización

Nivel de implentacion hasta la fecha	n	%
En proceso de desarrollo	1	16,7
Definido	2	33,3
Gestionado	3	50,0
Total	6	100,0
No contestaron	1	

Etapa II.2 Efectuar un análisis de riesgos

Nivel de implementación hasta la fecha	n	%
No implementado	1	16,7
Inicial	1	16,7
En proceso de desarrollo	1	16,7
Definido	2	33,3
Gestionado	1	16,7
Total	6	100,0
No contestaron	1	

Etapa II.3 En base a los controles establecidos para cada dominio de la norma, establecer la Brecha

Nivel de implentacion hasta la fecha	n	%
No implementado	1	16,7
Inicial	1	16,7
En proceso de desarrollo	2	33,3
Definido	1	16,7
Gestionado	1	16,7
Total	6	100,0
No contestaron	1	

Etapa III.1 Establecimiento del documento del plan a 1,2 o 3 años

Nivel de implentacion hasta la fecha	n	%
No implementado	1	16,7
Inicial	2	33,3
En proceso de desarrollo	2	33,3
Gestionado	1	16,7
Total	6	100,0
No contestaron	1	

Etapa III.2 Implementación del Plan de Seguridad dentro del POI

Nivel de implementación hasta la fecha	n	%
No implementado	1	16,7
Inicial	1	16,7
En proceso de desarrollo	1	16,7
Definido	2	33,3
Gestionado	1	16,7
Total	6	100,0
No contestaron	1	

Etapa IV.1 Política de Seguridad

Nivel de implementación hasta la fecha	n	%
En proceso de desarrollo	1	16,7
Definido	3	50,0
Gestionado	2	33,3
Total	6	100,0
No contestaron	1	

Etapa IV.2 Análisis de riesgos

Nivel de implementación hasta la fecha	n	%
No implementado	1	16,7
En proceso de desarrollo	3	50,0
Definido	2	33,3
Total	6	100,0
No contestaron	1	

Etapa IV.3 Brecha delo implementado y lo que falta por implementar

Nivel de implementación hasta la fecha	n	%
Inicial	1	16,7
En proceso de desarrollo	2	33,3
Definido	2	33,3
Gestionado	1	16,7
Total	6	100,0
No contestaron	1	

Etapa IV.4 Plan de Seguridad de la Información

Nivel de implementación hasta la fecha	n	%
No implementado	1	16,7
Inicial	1	16,7
En proceso de desarrollo	2	33,3
Definido	1	16,7
Gestionado	1	16,7
Total	6	100,0
No contestaron	1	

Grado de dificultad en implementación

Etapa I.1 Análisis e interpretación de los requerimientos de seguridad en base a la misión, visión y objetivos de la organización.

Grado de dificultad en implementacion	n	%
No hay dificultad	1	16,7
Algo de dificultad	2	33,3
Mediana dificultad	1	16,7
Alta dificultad	2	33,3
Total	6	100,0
No contestaron	1	

Etapa I.2 Identificación de los recursos (activos) dentro de los procesos de la organización

Grado de dificultad en implementacion	n	%
No hay dificultad	2	33,3
Algo de dificultad	1	16,7
Mediana dificultad	2	33,3
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa II.1 Establecimiento de la política de seguridad de la organización

Grado de dificultad en implementación	n	%
No hay dificultad	1	16,7
Algo de dificultad	3	50,0
Mediana dificultad	2	33,3
Total	6	100,0
No contestaron	1	

Etapa II.2 Efectuar un análisis de riesgos

Grado de dificultad en implementacion	n	%
Algo de dificultad	2	33,3
Mediana dificultad	3	50,0
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa II.3 En base a los controles establecidos para cada dominio de la norma, establecer la Brecha

Grado de dificultad en implementacion	n	%
Algo de dificultad	3	50,0
Mediana dificultad	2	33,3
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa III.1 Establecimiento del documento del plan a 1,2 o 3 años

Grado de dificultad en implementacion	n	%
Algo de dificultad	2	33,3
Mediana dificultad	4	66,7
Total	6	100,0
No contestaron	1	

Etapa III.2 Implementación del Plan de Seguridad dentro del POI

Grado de dificultad en implementacion	n	%
No hay dificultad	1	16,7
Algo de dificultad	2	33,3
Mediana dificultad	2	33,3
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa IV.1 Política de Seguridad

Grado de dificultad en implementacion	n	%
No hay dificultad	2	33,3
Algo de dificultad	2	33,3
Mediana dificultad	1	16,7
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa IV.2 Análisis de riesgos

Grado de dificultad en implementación	n	%
Algo de dificultad	3	50,0
Mediana dificultad	2	33,3
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa IV.3 Brecha delo implementado y lo que falta por implementar

Grado de dificultad en implementación	n	%
No hay dificultad	1	16,7
Algo de dificultad	2	33,3
Mediana dificultad	2	33,3
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Etapa IV.4 Plan de Seguridad de la Información

Grado de dificultad en implementación	n	%
Algo de dificultad	3	50,0
Mediana dificultad	2	33,3
Alta dificultad	1	16,7
Total	6	100,0
No contestaron	1	

Según su opinión la responsabilidad de la seguridad de la información en una organización es:

Ítem	n	%
De la alta dirección	4	25,0
De la gerencia de sistemas	3	18,8
Del gerente o jefe de área de la seguridad de la información	1	6,3
De todos los empleados	8	50,0
Total	16	100,0

Según su opinión para efectivizar el cumplimiento de la implementación de la norma la ONGEI:

Ítem	n	%
Debería realizar una auditoría de verificación de cumplimiento	5	31,3
Debe apoyar con consultorías especializadas	11	68,8
Total	16	100,0

III. Sobre el grado de influencia de los Factores Críticos en la implementación de la Norma Según su experiencia valore el grado de influencia de cada uno de los factores para la implementación de la Norma

a) Una política, objetivos y actividades que reflejen los objetivos de negocio de la organización.

Ítem	n	%
Algo de influencia	1	6,3
Mediana influencia	2	12,5
Alta influencia	4	25,0
Muy alta influencia	9	56,3
Total	16	100,0

b) Un enfoque para implantar, mantener y monitorear e improvisar la seguridad que sea consistente con la cultura de la organización.

Ítem	n	%
Mediana influencia	4	25,0
Alta influencia	11	68,8
Muy alta influencia	1	6,3
Total	16	100,0

c) El apoyo visible y el compromiso se la alta gerencia

Ítem	n	%
Mediana influencia	1	6,3
Alta influencia	5	31,3
Muy alta influencia	10	62,5
Total	16	100,0

d) La buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo.

Ítem	n	%
Mediana influencia	3	18,8
Alta influencia	8	50,0
Muy alta influencia	5	31,3
Total	16	100,0

e) La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados.

Ítem	n	%
Mediana influencia	1	6,3
Alta influencia	8	50,0
Muy alta influencia	7	43,8
Total	16	100,0

f) La distribución de guías sobre la política de seguridad de la información y de normas a todos los empleados y contratistas.

Ítem	n	%
Algo de influencia	2	12,5
Mediana influencia	6	37,5
Alta influencia	5	31,3
Muy alta influencia	3	18,8
Total	16	100,0

g) Aprovisionamiento para financiar actividades de gestión de la seguridad de la información.

Ítem	n	%
Algo de influencia	1	6,3
Mediana influencia	2	12,5
Alta influencia	11	68,8
Muy alta influencia	2	12,5
Total	16	100,0

h) La formación y capacitación adecuadas.

Ítem	n	%
Mediana influencia	1	6,3
Alta influencia	9	56,3
Muy alta influencia	6	37,5
Total	16	100,0

i) Establecer un efectivo proceso de gestión de incidentes de la seguridad de la información.

Algo de influencia	1	6,3
Mediana influencia	2	12,5
Alta influencia	10	62,5
Muy alta influencia	3	18,8
Total	16	100,0

j) Un sistema integrado y equilibrado de medidas que permita evaluar el rendimiento de la seguridad de la información y sugerir medidas.

Ítem	n	%
Mediana influencia	5	31,3
Alta influencia	8	50,0
Muy alta influencia	3	18,8
Total	16	100,0

k) Según su apreciación, las herramientas (Seguridad de la Información / Documentos / Plantillas) disponibles en el Portal de la ONGEI:

Ítem	n	%
Son muy útiles	6	42,9
Medianamente útil	8	57,1
Total	14	100,0
No contestaron	2	

ANEXO 5

FUNCIONES DE LOS ORGANISMOS PÚBLICOS DESCENTRALIZADOS ADSCRITOS A LA PRESIDENCIA DEL CONSEJO DE MINISTROS (PCM)

EL DESPACHO PRESIDENCIAL

El Despacho Presidencial o Casa de Gobierno es el organismo público encargado de administrar el pliego presupuestal creado mediante la Décima Disposición Complementaria y Transitoria de la Ley Nº 27573, Ley de Presupuesto del Sector Público para el año Fiscal 2002, con autonomía económica, financiera y administrativa. El Despacho Presidencial se encuentra adscrito al Sector de la Presidencia del Consejo de Ministros y tiene por sede la Casa de Gobierno en la ciudad de Lima.

Misión

Somos una institución, con autonomía económica, financiera y administrativa, que tiene por finalidad proporcionar la asistencia técnica y administrativa que requiere el señor Presidente de la República para el cumplimiento de sus responsabilidades y facultades que la Constitución Política, Leyes y demás disposiciones vigentes otorgan al Jefe de Estado.

Visión

Ser una institución sólidamente organizada, moderna, eficiente y transparente, con una cultura organizacional de honestidad y constante superación, con personal adecuado con valores morales, éticos e iniciativa de los mismos; que brinde asesoramiento, apoyo administrativo, y seguridad

integral al señor Presidente de la República, para el buen cumplimiento de sus funciones y atribuciones, que redunde en beneficio del país.

Funciones

1. Programar las actividades oficiales del Presidente de la República y, con su aprobación, realizar las coordinaciones para su ejecución.
2. Atender los gastos e inversiones correspondientes a la Presidencia de la República.
3. Asegurar el trámite fluido de la correspondencia del Presidente de la República.
4. Atender y apoyar al Presidente de la República en el desarrollo de sus diversas actividades, así como en sus relaciones con los organismos estatales, instituciones, entidades y sectores representativos de la ciudadanía.
5. Ejecutar las etapas administrativas que permitan la realización de las reuniones del Consejo de Ministros.
6. Coordinar el apoyo necesario para la seguridad del Presidente de la República y su familia, así como de los dignatarios, autoridades y otros visitantes de Palacio de Gobierno y velar por la conservación, mantenimiento y seguridad de dichas instalaciones.
7. Planificar, coordinar, conducir, monitorear, evaluar y controlar el desarrollo de las actividades de los órganos integrantes de la estructura orgánica del Despacho Presidencial.
8. Apoyar y difundir las actividades del Presidente de la República.
9. Otras funciones que le sean asignadas.

LA COMISIÓN NACIONAL PARA EL DESARROLLO Y VIDA SIN DROGAS (DEVIDA)

Misión

Diseñar y conducir las políticas contra las drogas en el país, en forma eficiente y concertada, coordinando, promoviendo, orientando programas y proyectos dirigidos con este fin, con la provisión oportuna de recursos del Estado y con el apoyo de la comunidad internacional, con el fin de lograr que la población peruana excluya acciones vinculadas a la producción, el consumo de drogas y privilegie estilos de vida saludables.

Visión

DEVIDA es modelo de institución rectora en el país, promotora, moderna, integrada y proactiva, reconocida por la comunidad internacional al haber logrado un real compromiso y una acción efectiva en la lucha contra las drogas de parte de los sectores, instituciones, gobiernos regionales y locales, así como de la sociedad civil, minimizando los factores socio económicos que incentivan la producción, tráfico y consumo de drogas en el Perú.

Funciones

a. Dirigir y coordinar el proceso de diseño de la Estrategia Nacional contra las Drogas y sus actualizaciones anuales.

b. Aprobar la Estrategia Nacional contra las Drogas y su actualización anual y los programas operativos anuales que la componen.

c. Coordinar el proceso de diseño y elaboración de los programas operativos anuales; dirigir y coordinar los procesos de monitoreo y evaluación de los

mismos, aprobando las medidas correctivas necesarias para alcanzar los resultados esperados.

d. Promover, coordinar y acordar con las diferentes instituciones del Estado, vinculadas a la lucha contra las drogas, los proyectos y actividades que se ejecutarán anualmente y promover la inclusión de éstas en el presupuesto Nacional.

e. Coordinar con las diferentes instituciones del Estado el diseño de las políticas sectoriales necesarias para consolidar y hacer sostenibles los logros que se alcancen en la lucha contra las drogas.

f. Promover la inversión privada en favor de la ejecución de los programas contenidos en la Estrategia Nacional contra las Drogas.

g. Convocar, coordinar y negociar en coordinación con el ministerio de Relaciones Exteriores, con la Comunidad Internacional el apoyo que requiere el Perú para implementar la Estrategia Nacional contra las Drogas.

h. Coordinar con el Ministerio de Relaciones Exteriores la política exterior del Perú en el ámbito de las drogas.

i. Las demás funciones que se le asigne por Ley.

DIRECCIÓN NACIONAL DE INTELIGENCIA

Visión

Constituirse en un organismo altamente especializado en Inteligencia Estratégica, con acciones eficaces y eficientes, de prestigio nacional e internacional, soporte importante para la toma de decisiones de las más altas autoridades del Estado en asuntos de Seguridad Nacional.

Misión

Producir inteligencia estratégica y ejecutar medidas de contrainteligencia en los campos no militares; así como, dirigir, coordinar, centralizar, integrar, procesar y difundir la inteligencia que le proveen obligatoriamente todos los componentes del SINA, para el proceso de toma de decisiones del Presidente Constitucional de la República y del Consejo de Ministros en materia de Seguridad Nacional.

Funciones

Funciones de la DINI como órgano rector del SINA (Art.24):

• Proveer al Presidente Constitucional de la República y al Consejo de Ministros, la inteligencia y la contrainteligencia necesaria, oportuna y predictiva.

• Dirigir, coordinar, centralizar, integrar, procesar y difundir la inteligencia producida por los componentes del Sistema de Inteligencia Nacional.

• Elaborar la propuesta de Plan Anual de Inteligencia.

• Articular los componentes del Sistema de Inteligencia Nacional.

• Informar periódicamente a la Comisión de Inteligencia del Congreso de la República sobre las actividades del SINA.

• Establecer y fortalecer las relaciones de cooperación con organismos similares de otros países.

• Formular, ejecutar y evaluar el pliego presupuestal.

EL INSTITUTO NACIONAL DE DEFENSA CIVIL (INDECI)

El Instituto Nacional de Defensa Civil (INDECI) es el organismo central, rector y conductor del Sistema Nacional de Defensa Civil, encargado de la organización de la población, coordinación, planeamiento y control de las actividades de Defensa Civil.

Visión

Organismo moderno, eficiente, eficaz y líder, en su rol de ente rector, normativo y conductor del Sistema Nacional de Defensa Civil en la prevención y atención de desastres; cuenta con la confianza y compromiso de las autoridades y población, contribuye al desarrollo sostenible del país, con prestigio internacional.

Misión

Regir y conducir el Sistema Nacional de Defensa Civil, formulando y promoviendo la implementación de políticas, normas, planes y programas para la prevención y atención de desastres, con la participación de autoridades y población; a fin de proteger la vida y el patrimonio, y contribuir al desarrollo sostenible del país.

Funciones

a. Proponer al Consejo de Defensa Nacional los objetivos y políticas de Defensa Civil.
b. Normar, coordinar, orientar y supervisar el planeamiento y la ejecución de la Defensa Civil.
c. Brindar atención de emergencia proporcionando apoyo inmediato a la población afectada por desastres.
d. Dirigir y conducir las actividades necesarias encaminadas a obtener la tranquilidad de la población.
e. Participar en la formulación y difusión de la doctrina de seguridad y Defensa Nacional en lo concerniente a Defensa Civil.
f. Asesorar al Consejo de Defensa Nacional en materia de Defensa Civil.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL (INDECOPI)

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) fue creado en noviembre de 1992, mediante el Decreto Ley N° 25868.

Tiene como funciones la promoción del mercado y la protección de los derechos de los consumidores. Además, fomenta en la economía peruana una cultura de leal y honesta competencia, resguardando todas las formas de propiedad intelectual: desde los signos distintivos y los derechos de autor hasta las patentes y la biotecnología.

El INDECOPI es un Organismo Público Especializado adscrito a la Presidencia del Consejo de Ministros, con personería jurídica de derecho público interno. En consecuencia, goza de autonomía funcional, técnica, económica, presupuestal y administrativa (Decreto Legislativo No 1033).

Como resultado de su labor en la promoción de las normas de leal y honesta competencia entre los agentes de la economía peruana, el INDECOPI es concebido en la actualidad, como una entidad de servicios con marcada preocupación por impulsar una cultura de calidad para lograr la plena satisfacción de sus clientes: la ciudadanía, el empresariado y el Estado.

Misión

Promover y garantizar la leal competencia, los derechos de los consumidores y la propiedad intelectual en el Perú, propiciando el buen funcionamiento del mercado, a través de la excelencia y calidad de su personal

Visión

Ser reconocidos como una institución pública líder en el Perú y América Latina que brinda sus servicios de manera oportuna, transparente y confiable, contribuyendo a generar una cultura de mercado y el bienestar en la sociedad.

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMATICA (INEI)

Visión

En el año 2012, el Perú cuenta con un ágil y eficiente sistema de coordinación, producción y difusión de información estadística confiable, oportuna y de calidad con cobertura de datos desagregada todo nivel político-administrativo, que contribuye eficazmente al diseño, implementación y evaluación de políticas públicas, programas y proyectos de desarrollo que impactan en el crecimiento económico, reducción de la pobreza y la conservación ambiental. Satisface plenamente los requerimientos de los usuarios del sector público y privado. La información estadística es de fácil acceso y su producción y difusión se realiza con el uso intensivo de las Tecnologías de Información más avanzadas.

Misión

El sistema Estadístico Nacional es la red de entidades del sector público a nivel central, regional y local que, bajo la rectoría del Instituto Nacional de Estadística – INEI, produce y difunde información estadística oficial, en forma integrada, coordinada, racionalizada bajo una normatividad técnica común, con el propósito de contribuir al diseño, monitoreo y evaluación de políticas públicas y al proceso de toma de decisiones de los agentes socio económicos y de la comunidad académica, con estadísticas oportunas, confiables y de calidad.

EL INSTITUTO DE RADIO Y TELEVISIÓN DEL PERÚ (IRTP)

Visión

Ser una institución de comunicación masiva, moderna, reconocida por todos los peruanos, por la calidad de sus programas audiovisuales y radiales, que garantizan el acceso a la cultura, el derecho a la educación, el sano entretenimiento y a la información permanente, interactiva y objetiva; a través de nuestra cobertura de radiodifusión que fortalece la identidad nacional, la democracia y la imagen del Perú en el mundo.

Misión

Somos la institución de Radio y Televisión del Estado encargada de producir, emitir y difundir, programas con contenidos de información periodística, edúcativa, cultural y de entretenimiento; a través de nuestra distribución nacional de la señal de radiodifusión, promoviendo las políticas nacionales y contribuyendo al bienestar de todos los peruanos.

EL CUERPO GENERAL DE BOMBEROS VOLUNTARIOS DEL PERÚ (CGBV)

Misión

El Cuerpo General de Bomberos Voluntarios del Perú es la autoridad competente en materia de prevención, control y extinción de incendios, realiza acciones de atención de accidentes vehiculares y emergencias médicas, rescate y salvataje de vidas expuestas a peligro. Brinda sus servicios de manera voluntaria a toda la comunidad debido a su vocación de servicio, sensibilidad social, entrega y disciplina.

Visión

El CGBVP es una Institución consolidada, científica y técnicamente preparada que cumple con su misión, con equipos y maquinarias modernas que permiten un accionar más rápido y efectivo, con personal voluntario capacitado mediante técnicas actualizadas. La difusión de las recomendaciones sobre accidentes y desastres disminuyó el riesgo de siniestros. El ámbito de acción del CGBVP abarca todo el territorio nacional, incluso las zonas que estaban desprotegidas.

SIERRA EXPORTADORA

Visión

Sierra con actividades económicas competitivas y sostenibles, integrada a los mercados nacionales e internacionales, con niveles de vida y bienestar de su población acorde con el desarrollo económico y social del país.

Misión

Promover, fomentar y desarrollar actividades económicas productivas en la sierra, que permitan a los productores articularse competitivamente a mercados nacionales e internacionales.

Objetivos

Objetivo 1**:** Desarrollar y consolidar el mercado Nacionales e Internacional.
Objetivo 2**:** Consolidar y Ampliar una oferta competitiva de productos en la Sierra peruana en función de la demanda real nacional e internacional.
Objetivo 3**:** Facilitar el acceso a recursos y servicios financieros e inversiones para el desarrollo de negocios y proyectos productivos.
Objetivo 4**:** Coordinación y formulación de políticas públicas y promoción de mecanismos de desarrollo territorial

CENTRO NACIONAL DE PLANEAMIENTO ESTRATEGICO – CEPLAN

Misión

Impulsar la instauración de una cultura de planeamiento estratégico concertado en los diferentes niveles de gobierno, asegurando que las acciones del Estado alcancen los objetivos nacionales de desarrollo e integración a la economía global y la mejora de la gestión pública.

Visión

El CEPLAN al 2011, es reconocido por la sociedad como la institución que lidera el proceso de construcción de una visión compartida y concertada de futuro de país, y que construye escenarios de futuro, para integrar al país en la dinámica de los mercados globales.
Asimismo, ha consolidado un Sistema Nacional de Planeamiento Estratégico, dinámico y eficaz, que formula, hace seguimiento y actualiza los planes estratégicos en los diferentes niveles de gobierno del Estado.

Funciones

1. Constituirse en el espacio institucionalizado para la definición concertada de una visión de futuro compartida y de los objetivos y planes estratégicos para el desarrollo nacional armónico, sustentable, sostenido y descentralizado del país.

2. Articular e integrar en forma coherente y concertada las diferentes propuestas y opiniones para la elaboración del Plan Estratégico de Desarrollo Nacional y los planes nacionales, sectoriales, institucionales y subnacionales, así como las orientaciones, los métodos, los procesos y los instrumentos para el planeamiento estratégico.

3. Promover y articular los programas de fortalecimiento de capacidades para el planeamiento estratégico.

4. Desarrollar los procesos y las acciones para el monitoreo de la gestión para resultados de mediano y largo plazo, en coordinación con el Consejo Nacional de Competitividad, basada en los diferentes instrumentos de planeamiento estratégico y con orientación hacia la promoción de la modernización administrativa y el logro de estándares de eficiencia al servicio del ciudadano, así como de la mejora de los índices de competitividad del país para aprovechar las oportunidades que la dinámica internacional ofrece en el marco de los tratados internacionales de promoción, asociación y cooperación económica y comercial de los que el Perú es parte.

5. Promover la cooperación y acuerdos entre los sectores público y privado en el proceso de formulación de los planes estratégicos nacionales, sectoriales, institucionales y sub nacionales, así como en la ejecución de los programas y proyectos priorizados en esos ámbitos, para asegurar el desarrollo nacional y la mejora constante de la competitividad del país.

6. Promover la formulación de planes estratégicos, programas y proyectos con visión prospectiva de mediano y largo plazo, así como el desarrollo de los aspectos teóricos que los sustentan, aplicando un enfoque nacional contextualizado en el ámbito internacional, con prioridad en las relaciones y oportunidades que tienen su origen en los acuerdos internacionales de los que el Perú es parte.

LA AUTORIDAD NACIONAL DEL SERVICIO CIVIL – SERVIR

Organismo con personería jurídica de derecho público interno y con autonomía técnica adscrito a la Presidencia del Consejo de Ministros. El objetivo de SERVIR es ejercer la rectoría del sistema administrativo de gestión de los recursos humanos del sector público (incluidas las entidades de la administración central, los gobiernos regionales y locales).

Misión

Mejorar el servicio civil de manera integral y continua para servir al ciudadano.

Visión

SERVIR lidera procesos de reforma del servicio civil, es reconocida por los actores clave, en especial por los ciudadanos a partir de sus resultados y forma parte del núcleo estratégico de decisión del Estado.

***Funciones*:**

1. Desarrollar Oficinas de Recursos Humanos descentralizadas, que actúan como socios estratégicos cercanos a la gente;
2. Apoyar a la modernización facultativa de los gobiernos regionales y locales;
3. Implementar y gestionar el Cuerpo de Gerentes Públicos a ser destacados a entidades de los tres niveles de gobierno;
4. Establecer los lineamientos para la capacitación y mejora del rendimiento de los servidores públicos y la eficiencia de los servicios que brinda el Estado;
5. Desarrollar un sistema de evaluación e información;
6. Desarrollar programas piloto de evaluación, para asegurar los métodos a usar según los distintos tipos de entidades y, sobre todo, los tipos de tareas específicas que desempeña cada servidor;
7. Proponer la política remunerativa, que incluye la aplicación de incentivos monetarios y no monetarios vinculados al rendimiento;
8. Resolver de forma progresiva conflictos individuales en materias relativas al acceso al servicio civil, pago de retribuciones, evaluación y progresión en la carrera, régimen disciplinario y terminación de la relación laboral, a través del Tribunal del Servicio Civil, que constituye la última instancia de la vía administrativa.

ORGANISMO DE SUPERVISIÓN DE LOS RECURSOS FORESTALES Y DE FAUNA SILVESTRE (OSINFOR)

Misión

OSINFOR es la autoridad nacional, encargada de gestionar eficaz, eficiente, y oportunamente, la supervisión y fiscalización del aprovechamiento de los recursos forestales, fauna silvestre y los servicios ambientales provenientes del bosque, estableciendo alianzas estratégicas con los diferentes actores involucrados, que permitan el crecimiento sostenible y el posicionamiento del Perú entre los países más competitivos.

Visión

OSINFOR líder en supervisar y fiscalizar el aprovechamiento sostenible de los recursos forestales, fauna silvestre y los servicios ambientales provenientes del bosque, contribuye al crecimiento sostenible del Perú y colabora activamente a posicionar al Perú entre los 15 países más competitivos del orbe.